IBM eMessage
Version 9 Release 1
13. Februar 2015

Einrichtungs- und Administratorenhandbuch

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 129 gelesen werden.

Diese Ausgabe bezieht sich auf Version 9, Release 1, Modifikation 0 von IBM eMessage und alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM eMessage, Version 9 Release 1, Startup and Administrators Guide,
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 1999, 2015

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
TSC Germany
Kst. 2877
Februar 2015

© Copyright IBM Corporation 1999, 2015.

Inhaltsverzeichnis

Kapitel 1. Gehostetes Messaging mit IBM Campaign und IBM eMessage . . . 1

Einrichten eines gehosteten E-Mail-Kontos bei IBM . 1
Übersicht über den Startprozess 1
Vorbereitungen für die Arbeit mit eMessage 3

Kapitel 2. Konfigurieren der lokalen IBM EMM-Umgebung für eMessage 5

eMessage-Funktionen in Campaign aktivieren . . . 5
eMessage-Registrierung bestätigen 5
Anzeigen von eMessage-Menüoptionen 6
Merkmale der eMessage-Systemtabellen angeben . . 7
Zugriff auf eMessage-Systemtabellen konfigurieren . 8
Konfiguration des Zugriffs auf lokale eMessage-Systemtabellen. 8
Erforderliche Zuordnung für eMessage-Systemtabellen in Campaign 9
Erforderlicher Neustart des Webanwendungsservers für Campaign 9

Kapitel 3. Verbindungen zu gehosteten E-Mail-Services 11

Anforderungen für die Konfiguration einer Verbindung zu IBM EMM Hosted Services 11
Voraussetzungen für den Upload von Daten in IBM EMM Hosted Services 12
Verbindungs- und Portanforderungen 12
Standard-Uploadverbindung über explizites FTP 13
Daten mit implizitem FTP hochladen 14
Verbindungsaufbau über einen HTTP-Proxy . . 17
Downloadrate für Daten und Porteinstellung . . . 23
Anforderung für den Systembenutzer für den Zugriff auf IBM EMM Hosted Services 23
Systembenutzer mit Zugriff auf IBM EMM Hosted Services konfigurieren 24
Konfigurieren der Adressen zur Verbindungsherstellung mit IBM EMM Hosted Services 25
Adressen zum Herstellen einer Verbindung zu IBM EMM Hosted Services konfigurieren . . . 25
Konfigurieren der sicheren Kommunikation für gehostete E-Mail 26
Generieren eines vertrauenswürdigen Keystores 27
Konfigurieren von SSL bei Verwendung von WebLogic 28
Konfigurieren von SSL bei Verwendung von IBM WebSphere 31

Kapitel 4. RCT (Response and Contact Tracker) 35

RCT manuell starten 35
Manueller Betrieb des RCT (Response and Contact Tracker) 36
Response and Contact Tracker stoppen 36
Informationen zum automatischen Starten des RCT als Service 36
Response and Contact Tracker als Service hinzufügen 37
RCT-Service entfernen 38

Kapitel 5. Überprüfung beim Start . . . 39

Prüfung der Systemkonfigurationen 39
Upload an IBM EMM Hosted Services testen . . . 41
Download aus IBM EMM Hosted Services testen . . 41
Verbindung mit der gehosteten Messaging-Schnittstelle testen 41

Kapitel 6. Konfigurationen für IBM eMessage 43

Für eMessage zu konfigurierende Aspekte 44
Nach Konfigurationsänderungen erneut zu startende Komponenten 45
Zugriff auf zusätzliches Protokoll der Mailing-Ausführung konfigurieren 46
Unterstützung für die Integration von Campaign-Angeboten. 47
Konfigurieren der Unterstützung für Dimensionstabellen 47
Konfiguration des Zugriffs auf lokale eMessage-Systemtabellen 48
Konfigurationseigenschaften für eMessage 48
Campaign | Partitionen | Partition[n] | eMessage 49
Campaign | Partitionen | Partition[n] | Server | intern 50
Campaign | Partitionen | Partition[n] | eMessage | contactAndResponseHistTracking . . . 53
eMessage | serverComponentsAndLocations | hostedServices 55
eMessage | Partitionen | Partition[n] | hostedAccountInfo. 56
eMessage | Partitionen | Partition[n] | dataSources | systemTables 57
eMessage | Partitionen | Partition[n] | recipientListUploader 60
eMessage | partitions | partition[n] | responseContactTracker 60

Kapitel 7. Konfigurationen für die Implementierung mobiler IBM Push-Benachrichtigungen 63

Überblick über die Integration mobiler Apps in IBM Messaging-Systeme. 63
Integration von Google Cloud Messaging in IBM eMessage 64
Voraussetzungen für die Integration von Google Android-Apps in IBM Push-Benachrichtigungen . 64

© Copyright IBM Corp. 1999, 2015

IBM Push Notification SDK for Android in Ihrer App implementieren 65
Einen App-Eingang für Android-Apps bereitstellen 67
Positionsgesteuerte Benachrichtigungen für Android-Apps bereitstellen 68
Benachrichtigungen zu Aktionszielen bereitstellen 70
Unterstützung für Ereignisse und Benachrichtigungen konfigurieren 70
Benachrichtigungen anpassen 73
Die Benutzer-ID einer mobilen App (XID) für Android integrieren 75
Integration des Apple Push Notification Service in IBM eMessage 75
Voraussetzungen für die Integration von Apple iOS-Apps in IBM Push-Benachrichtigungen. . . 76
iOS in Ihrer App implementieren 76
Einen App-Eingang für iOS-Apps bereitstellen. . 79
Aktionen in Benachrichtigungen bereitstellen . . 82
Positionsgesteuerte Benachrichtigungen für iOS Apps 85
Das SDK für positionsgesteuerte Benachrichtigungen konfigurieren 86
Benutzerdefiniertes Badge-Verhalten konfigurieren 87
Eine Push-Benachrichtigung für die Apple iOS-Beispiel-App erstellen 87
Alle Benachrichtigungen vom mobilen Gerät löschen 88
App-Registrierungsbenachrichtigung erhalten . . 88
Die Benutzer-ID einer mobilen App (XID) für iOS integrieren. 88
Gehostetes Messaging-Konto für mobiles Messaging aktivieren 89
Mobile App in IBM eMessage registrieren 90
Anforderung zur Identifikation von App-Benutzern in der Marketing-Datenbank. 91
Integration der mobilen App auf einem mobilen Gerät testen 92
Positionen für die Zustellung nach Positions-Triggering konfigurieren 93
Positionseigenschaften bearbeiten 93
Verfügbare Positionen für die Zustellung nach Positions-Triggering löschen 94
Standardwerte für mobiles Messaging konfigurieren 94
Push-Benachrichtigung-Aufzeichnungsdaten von IBM 95

Kapitel 8. Dienstprogramme für eMessage. 97
RLU-Script 97
eMessage-Script für den Response and Contact Tracker (RCT). 98
eMessage-Script 'MKService_rct' 99
configTool 100
Sichern von Konfigurationseinstellungen . . . 104

Kapitel 9. Informationen zur Fehlersuche bei eMessage 107
Protokolldateien für eMessage. 107
Verwenden von log4j mit eMessage 107

Kapitel 10. Verwaltung des Benutzerzugriffs auf Messaging-Funktionen . . 109
Rollen- und Richtlinienzuweisung für Mailing-Zugriff 109
Rollen und Berechtigungen in Marketing Platform und Campaign 110
Informationen zu Sicherheitsrichtlinien 110
Nachrichtenberechtigungen in Campaign 112
Rollen und Berechtigungen zur Verfügung stellen 113
Evaluierung von Berechtigungen in Campaign 114
Definition der Berechtigungsstatus 114
Berechtigungen für Mailings in Campaign. . . 115
Berechtigungen für die Kategorie 'Digitale Assets' 116
Berechtigungen für die Kategorie 'Dokumente' 117
Berechtigungen für die Kategorie 'E-Mail-Verwaltung' 117
Nachrichtenberechtigungen für eMessage 118
eMessage-Rollen zuweisen 119
E-Mail-Domänen und Kurzlinkdomänen 119
Wartung von gehosteten E-Mail-Domänen. . . 120
Standardabsenderadresse und Anzeigenamen konfigurieren. 121
Steuerung des Zugriffs auf die Liste gesendeter Nachrichten 122
Zugriff auf die Liste gesendeter Nachrichten erteilen 123
Zugriff auf die Liste gesendeter Nachrichten verweigern 124
Einschränkung für die Liste gesendeter Nachrichten aktivieren 125
Berechtigungen für eMessage-Berichte 126

Bevor Sie sich an den IBM Technical Support wenden 127

Bemerkungen 129
Marken 131
Hinweise zu Datenschutzrichtlinien und Nutzungsbedingungen 131

Kapitel 1. Gehostetes Messaging mit IBM Campaign und IBM eMessage

Wenn Sie IBM® Campaign in IBM eMessage integrieren, können Sie mithilfe von eMessage Marketing-Kampagnen mit hochgradig personalisierten E-Mails durchführen.

eMessage bietet Zugriff auf durch IBM gehostete Ressourcen. Dies ermöglicht es Ihnen, angepasste Nachrichten basierend auf den in Ihrem Kunden-Datamart gespeicherten Informationen zu entwerfen, zu senden und einzeln zu überwachen.

- In Campaign können Sie Ablaufdiagramme verwenden, um Listen mit E-Mail-Empfängern zu erstellen und Personalisierungsdaten für jeden Empfänger auszuwählen.
- In eMessage können Sie durch IBM gehostete Ressourcen für E-Mail-Design, -Übertragung und -Zustellbarkeit verwenden, um E-Mail-Marketing-Kampagnen durchzuführen.

Einrichten eines gehosteten E-Mail-Kontos bei IBM

Wenn Sie ein eMessage-Abonnement erwerben, erstellt IBM ein gehostetes E-Mail-Konto für Sie und sendet Ihnen die zugehörigen Berechtigungsnachweise, die Sie benötigen, um die eMessage-Funktionen zu nutzen. Sie verwenden diese Berechtigungsnachweise beim Konfigurieren Ihrer lokalen IBM EMM-Anwendungen, um über sichere Verbindungen auf die gehostete E-Mail-Umgebung zuzugreifen.

Sie müssen ein gültiges Konto besitzen, um auf die E-Mail-Ressourcen zuzugreifen, die IBM als Software-Service bereitstellt. Wenn Ihre IBM EMM-Installation mehrere Partitionen enthält, und Sie planen, eMessage in mehreren Partitionen zu verwenden, benötigen Sie ein gehostetes E-Mail-Konto für jede Partition. E-Mail-Konten können nicht installations- oder partitionsübergreifend gemeinsam genutzt werden.

Die Erstellung eines gehosteten E-Mail-Kontos stellt den Beginn des Startprozesses dar, der ungefähr 90 Tage dauert. Eine allgemeine Beschreibung des Prozesses finden Sie unter „Übersicht über den Startprozess”.

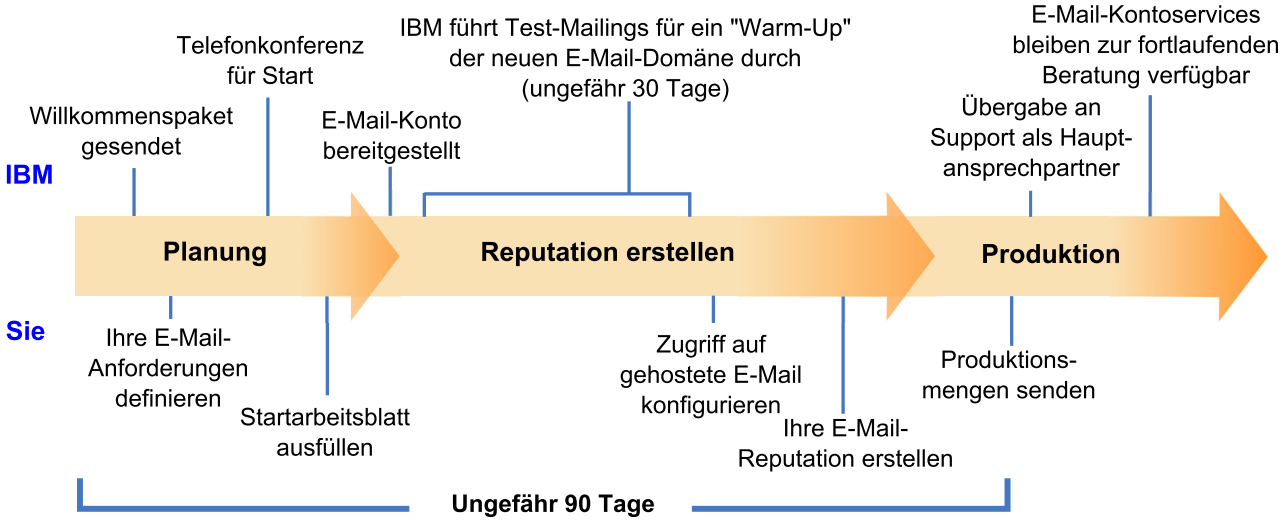
Übersicht über den Startprozess

Sie können E-Mail-Funktionen in IBM Campaign aktivieren, um hochgradig zielgerichtete und verfolgbare E-Mail-Marketing-Kampagnen durchzuführen. Campaign verwendet E-Mail Funktionen, die von IBM eMessage über Ressourcen bereitgestellt werden, die in Rechenzentren in den USA und Großbritannien gehostet werden. Ein Konto für den Zugriff auf diese Ressourcen ist in Ihrem eMessage-Abonnement enthalten.

IBM beginnt den Startprozess, nachdem Ihr gehostetes E-Mail-Konto erstellt wurde. IBM unterstützt Sie dabei, sich mit eMessage vertraut zu machen, die Verbindung zu gehosteten E-Mail-Ressourcen herzustellen und sich eine Reputation als legitimer E-Mail-Marketer unter führenden Internet-Service-Providern (ISPs) zu schaffen.

Der Prozess verläuft in drei Phasen. Die Professional Services- und Email Account Services-Teams von IBM begleiten Sie unterstützend durch den gesamten Prozess.

© Copyright IBM Corp. 1999, 2015



Der Professional Services-Berater ist Ihr Hauptansprechpartner bei IBM während des Startprozesses. Wenn der Konto-Startprozess abgeschlossen ist, überträgt der Professional Services-Berater die Hauptzuständigkeit für den Support auf das IBM Produktunterstützungsteam.

Ein fest zugeordneter EAS-Berater bietet spezielle Unterstützung bei E-Mail-Problemen. Die Schaffung einer positiven E-Mail-Reputation unter wichtigen Internet-Service-Providern ist entscheidend dafür, dass Ihre E-Mail-Marketing-Kampagnen stets Ihre Zielempfänger erreichen. Wenn Sie mit der Durchführung von Mailings beginnen, überprüft der EAS-Berater die Mailing-Zustellbarkeitsleistung und schlägt optimale Methoden für den allmählichen Aufbau Ihrer E-Mail-Reputation vor.

Startaktivitäten und Meilensteine

Planung

Aktion	Zuständige Stelle
Senden der Berechtigungsnachweise für das E-Mail-Konto und des Willkommenspakets, einschließlich Arbeitsblatt für den E-Mail-Start.	IBM Email Account Services
Planen einer Konferenzverbindung, um alle beteiligten Teilnehmer vorzustellen, Überprüfen des Startplans und Erläutern der E-Mail-Marketing-Ziele.	IBM Professional Services
Ausfüllen des Arbeitsblatts für den E-Mail-Start, um Ihre Anforderungen an die E-Mail-Domäne und Ihre Mailing-Prognosen zu definieren.	Ihre Organisation

Einrichtung Ihrer E-Mail-Reputation

Aktion	Zuständige Stelle
Bereitstellen des E-Mail-Kontos anhand der Informationen, die während der Konferenzverbindung und im Arbeitsblatt für den E-Mail-Start angegeben wurden.	IBM E-Mail-Operationen

Aktion	Zuständige Stelle
Senden erster Aufwärm-Mailings an ausgewählte Testkonten wichtiger ISPs. Bis zum Abschluss dieser Phase dauert es ungefähr 30 Tage.	IBM E-Mail-Operationen
Aktivieren von eMessage in IBM Campaign.	Ihre Organisation (mit Unterstützung durch IBM)
Konfigurieren des Zugriffs auf gehostete E-Mail-Ressourcen. Rücksprache mit EAS-Berater, welches Rechenzentrum angegeben werden soll.	Ihre Organisation (mit Unterstützung durch IBM)
Beginn des Sendens von Mailings. Um eine positive E-Mail-Reputation aufzubauen, senden Sie anfangs nur Mailings geringen Umfangs, denen Sie im Laufe der Zeit umfangreichere und häufigere Mailings folgen lassen. ISPs versuchen häufig, Spam zu begrenzen, indem sie umfangreiche oder häufige Mailings von E-Mail-Domänen blockieren, die nicht als berechtigt erkannt werden.	Ihre Organisation (mit Unterstützung durch IBM)
Bereitstellen von Zustellbarkeitsergebnissen und Reputationsberatung mit allmählich steigender Mailing-Menge und -Häufigkeit.	IBM Email Account Services

Produktion

Aktion	Zuständige Stelle
Senden von Mailings mit typischer Menge und Häufigkeit.	Ihre Organisation
Übertragen der Zuständigkeit für den Erstkontakt an das IBM Support-Team.	IBM Professional Services
Fortgesetztes Beratungsengagement bei E-Mail-Problemen. Regelmäßiger Kontakt für fortlaufenden E-Mail-Konto-Support.	IBM Email Account Services

Vorbereitungen für die Arbeit mit eMessage

Bevor Sie mit dem Startprozess für gehostetes E-Mail beginnen, beachten Sie die folgenden Punkte.

- Einige Konfigurationen erfordern einen Neustart des Webanwendungsservers. Planen Sie eMessage-Konfigurationsaktivitäten ein, um zu verhindern, dass es durch die Ausführung großer Ablaufdiagramme und anderer Aktivitäten in Campaign zu Konflikten kommt.
- IBM fordert Sie auf, eine Person zu benennen, die während des Startprozesses als primärer Ansprechpartner dient.
- Fordern Sie Berechtigungsnachweise für Ihr gehostetes E-Mail-Konto an, bevor Sie mit dem Startprozess beginnen. Sie verwenden diese Berechtigungsnachweise, um Ihre Systeme für den Zugriff auf das Konto zu konfigurieren.
- Beraten Sie sich mit Ihrem Netzadministrationspersonal. eMessage benötigt bestimmte Portbereiche für die Kommunikation mit IBM EMM Hosted Services.
- Vergewissern Sie sich, dass Sie über die entsprechenden Netzberechtigungen verfügen, um Konfigurationsänderungen vornehmen zu können.

Kapitel 2. Konfigurieren der lokalen IBM EMM-Umgebung für eMessage

Die Verwendung von eMessage zum Senden gehosteter E-Mail-Nachrichten erfordert Änderungen in der lokalen Installation von IBM EMM. Führen Sie die in den folgenden Abschnitten beschriebenen Schritte durch.

- „eMessage-Funktionen in Campaign aktivieren"
- „eMessage manuell registrieren" auf Seite 6
- „Merkmale der eMessage-Systemtabellen angeben" auf Seite 7
- „Erforderliche Zuordnung für eMessage-Systemtabellen in Campaign" auf Seite 9
- „Konfiguration des Zugriffs auf lokale eMessage-Systemtabellen" auf Seite 8
- „Erforderlicher Neustart des Webanwendungsservers für Campaign" auf Seite 9

Wenn Ihre Umgebung mehrere Partitionen enthält, wiederholen Sie diese Schritte für jede Campaign-Partition, in der Sie IBM eMessage verwenden. Weitere Informationen zum Erstellen von und Arbeiten mit mehreren Partitionen finden Sie im *IBM Campaign-Installationshandbuch*.

eMessage-Funktionen in Campaign aktivieren

Bei der Installation von Campaign installiert das Installationsprogramm auch eMessage in der Standardpartition, aktiviert es jedoch nicht. Die Funktionen von eMessage sind erst verfügbar, wenn Sie eMessage aktivieren.

Vorbereitende Schritte

Überprüfen Sie, ob eMessage ordnungsgemäß bei IBM Marketing Platform registriert wurde.

Die Registrierung von eMessage bei Marketing Platform ist Teil des Installationsprozesses für IBM Campaign.

Vorgehensweise

1. Bearbeiten Sie in IBM Marketing Platform die Angaben für `Campaign > partitions > partition[n] > server > internal > eMessageInstalled`.
2. Um eMessage zu aktivieren, ändern Sie den Wert in `yes`.

Zugehörige Tasks:

„eMessage-Registrierung bestätigen"

eMessage-Registrierung bestätigen

IBM eMessage muss in IBM Marketing Platform registriert werden. Um festzustellen, dass eMessage erfolgreich registriert wurde, müssen Sie die Konfiguration für Marketing Platform überprüfen.

© Copyright IBM Corp. 1999, 2015

Vorgehensweise

1. Melden Sie sich bei IBM EMM an.
2. Navigieren Sie zu **Einstellungen** > **Konfiguration**.
3. Suchen Sie nach der Konfigurationskategorie eMessage.

   Wenn IBM eMessage bei Marketing Platform registriert ist, wird die Kategorie eMessage in der Hierarchie der Konfigurationseigenschaften angezeigt.

Nächste Schritte

Wenn die Kategorie eMessage nicht in der Eigenschaftenhierarchie angezeigt wird, lesen Sie im *IBM Campaign-Installationshandbuch* nach, wie Sie eMessage manuell registrieren können.

Wenn die eMessage-Kategorie verfügbar ist, müssen Sie die eMessage-Funktionen in Campaign aktivieren.

Zugehörige Tasks:

„eMessage-Funktionen in Campaign aktivieren" auf Seite 5

eMessage manuell registrieren

Wenn das Installationsprogramm von eMessage während der Installation nicht auf die Marketing Platform-Systemtabellen zugreifen kann, müssen Sie das Dienstprogramm **configTool** ausführen, um die Registrierung manuell durchzuführen.

Informationen zu diesem Vorgang

Das Installationsprogramm von Campaign registriert eMessage normalerweise automatisch zusammen mit den Marketing Platform-Systemtabellen, ohne dass eMessage aktiviert wird. In einigen Situationen stellt das Campaign-Installationsprogramm keine Verbindung zu den Marketing Platform-Systemtabellen her, um eMessage automatisch zu registrieren.

Wenn das Installationsprogramm eMessage nicht automatisch registriert, müssen Sie eMessage manuell mit dem Dienstprogramm `configTool` registrieren, das mit der IBM EMM-Installation bereitgestellt wird.

Vorgehensweise

1. Navigieren Sie in der Marketing Platform-Installation zum Verzeichnis `tools\bin`.

   Das Dienstprogramm `configTool` befindet sich im Verzeichnis `tools\bin`. Das eMessage-Installationsverzeichnis ist ein Unterverzeichnis des Campaign-Installationsverzeichnisses.
2. Führen Sie den Befehl **configTool -r eMessage -f "*vollständiger Pfad zum eMessage-Installationsverzeichnis*\conf\emessage_configuration.xml"** aus.

Anzeigen von eMessage-Menüoptionen

Um IBM eMessage nutzen zu können, müssen Sie die Systemkonfiguration aktualisieren, sodass Menüoptionen für eMessage in der Benutzeroberfläche von IBM Marketing Platform angezeigt werden. Verwenden Sie zum Anzeigen der erforderlichen Optionen das mit Ihrer IBM EMM-Installation bereitgestellte Dienstprogramm `configTool`.

Sie müssen `configTool` mit bestimmten Parametern für jede eMessage-Menüoption ausführen. Durch die Ausführung von `configTool` werden Systemkonfigurationseinstellungen aktualisiert. Sie müssen den Webanwendungsserver erneut starten, um die Änderungen zu übernehmen. eMessage wird zwar mit Campaign installiert, aber die Menüoptionen für eMessage werden erst angezeigt, nachdem Sie `configTool` ausgeführt und den Webanwendungsserver erneut gestartet haben. Das Dienstprogramm `configTool` befindet sich im Ordner `bin` im Verzeichnis `tools` der Marketing Platform-Installation.

Anmerkung: Sie müssen einen Pfad zum eMessage-Installationsverzeichnis als `configTool`-Parameter angeben. Das eMessage-Installationsverzeichnis ist ein Unterverzeichnis des Campaign-Installationsverzeichnisses.

- **eMessage-Einstellungen** im Menü **Einstellungen** anzeigen

  ```
  configTool.bat -v -i -p "Affinium|suite|uiNavigation|settingsMenu" -f
  "vollständiger Pfad zum eMessage-Installationsverzeichnis\conf\
  emessage_op_odsettings_navigation.xml"
  ```

- **eMessage-Mailings** im Menü **Kampagne** anzeigen

  ```
  configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu|Campaign"
  -f "vollständiger Pfad zum eMessage-Installationsverzeichnis\conf\
  emessage_op_mailings_navigation.xml"
  ```

- **eMessage-Dokumente** im Menü **Kampagne** anzeigen

  ```
  configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu|Campaign"
  -f "vollständiger Pfad zum eMessage-Installationsverzeichnis\conf\
  emessage_op_documents_navigation.xml"
  ```

- **eMessage-Analysen** im Menü **Analyse** anzeigen

  ```
  configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu|Analytics"
  -f "vollständiger Pfad zum eMessage-Installationsverzeichnis\conf\
  emessage_op_analytics_navigation.xml"
  ```

Überprüfen Sie anschließend, ob die Menüoptionen erfolgreich hinzugefügt wurden: Melden Sie sich nach dem Neustarten des Webanwendungsservers bei IBM EMM an, öffnen Sie die Menüs **Einstellungen**, **Kampagne** und **Analyse**, und stellen Sie fest, ob die eMessage-Optionen angezeigt werden.

Merkmale der eMessage-Systemtabellen angeben

IBM eMessage benötigt Informationen, die den Typ, das Schema und die JDBC-Verbindung für die eMessage-Systemtabellen in Ihrer Installation beschreiben. Die eMessage-Systemtabellen werden im Campaign-Schema als Teil des Campaign-Installationsprozesses erstellt.

Vorgehensweise

Geben Sie in den folgenden Konfigurationseigenschaften die erforderlichen Informationen an. Ausführliche Informationen zum Festlegen der Konfigurationseigenschaften finden Sie in der Marketing Platform-Onlinehilfe zu den einzelnen Eigenschaften.

- `eMessage > partitions > partition [n] < dataSources > systemTables > type`
- `eMessage > partitions > partition [n] < dataSources > systemTables > schemaName`
- `eMessage > partitions > partition [n] < dataSources > systemTables > jdbcBatchSize`

- `eMessage > partitions > partition [n] < dataSources > systemTables > jdbcClassName`
- `eMessage > partitions > partition [n] < dataSources > systemTables > jdbcURI`

Nächste Schritte

Weitere Informationen zu Konfigurationseigenschaften und zum Konfigurieren von eMessage finden Sie in Kapitel 6, „Konfigurationen für IBM eMessage", auf Seite 43.

Zugriff auf eMessage-Systemtabellen konfigurieren

eMessage-Komponenten müssen ohne manuelle Benutzereingabe automatisch auf Systemtabellen zugreifen können. Damit eMessage-Komponenten auf Systemtabellen im Campaign-Schema zugreifen können, ohne dass eine manuelle Datenbankanmeldung erforderlich ist, definieren Sie in IBM Marketing Platform einen Systembenutzer. Sie müssen diesen Systembenutzer konfigurieren, um die Zugriffsberechtigungen für die Datenbank bereitzustellen, in der das Campaign-Schema enthalten ist.

Systembenutzer und Datenquellen werden in IBM Marketing Platform konfiguriert. Weitere Informationen zum Erstellen von Systembenutzern und Datenquellen finden Sie im *IBM Marketing Platform-Administratorhandbuch*.

Konfiguration des Zugriffs auf lokale eMessage-Systemtabellen

IBM eMessage erfordert den Zugriff auf die eMessage-Systemtabellen im Campaign-Schema. Damit eMessage-Komponenten ohne manuelle Datenbankanmeldung auf Systemtabellen im Campaign-Schema zugreifen können, müssen Sie einen eMessage-Systembenutzer angeben, um die erforderlichen Berechtigungsnachweise für den Datenbankzugriff bereitzustellen.

Informationen zu diesem Vorgang

Der Systembenutzer, der auf die Datenbank zugreift, ist einer IBM Marketing Platform-Datenquelle zugeordnet, die die Berechtigungsnachweise für die Anmeldung an der Datenbank enthält, in der sich das Campaign-Schema befindet.

Weitere Informationen zu Konfigurationseigenschaften für Systemtabellen finden Sie im Abschnitt „eMessage | Partitionen | Partition[n] | dataSources | systemTables" auf Seite 57.

Vorgehensweise

1. Geben Sie den Systembenutzer an, den Sie in IBM Marketing Platform definiert haben. Bearbeiten Sie dazu die folgende Konfigurationseigenschaft:

   `eMessage > partitions > partition [n] < dataSources > systemTables > asmUserForDBCredentials`
2. Geben Sie die Berechtigungsnachweise für die Anmeldung an der Datenbank an, die das Campaign-Schema und die eMessage-Systemtabellen enthält. Bearbeiten Sie dazu die folgende Konfigurationseigenschaft:

   `eMessage > partitions > partition [n] < dataSources > systemTables > amDataSourceForDBCredentials`

Erforderliche Zuordnung für eMessage-Systemtabellen in Campaign

Sie müssen eMessage-Systemtabellen im Campaign-Schema entsprechenden eMessage-Datenbanktabellen zuordnen. Die eMessage-Systemtabellen haben **eMessage** im Tabellennamen.

Ordnen Sie in Campaign die folgenden eMessage-Systemtabellen zu.

- eMessage-Ausgabelistentabelle
- eMessage-Ausgabeliste-Zielgruppenfelder-Zuordnungstabelle
- eMessage-Mailing-Tabelle
- eMessage-Mailing-Instanz-Tabelle
- eMessage-Datentabellenspalten-Zuordnungstabelle
- eMessage-Personalisierungsfeld-Zuordnungstabelle
- eMessage-Personalisierungsfeld-Nutzungstabelle

Informationen zum Zuordnen von Tabellen finden Sie im *IBM Campaign-Administratorhandbuch*.

Erforderlicher Neustart des Webanwendungsservers für Campaign

Nachdem Sie Änderungen an den Konfigurationen von Campaign und eMessage vorgenommen haben, müssen Sie den Webanwendungsserver erneut starten, auf dem sich Campaign befindet.

Eine Anleitung zum erneuten Starten finden Sie in der Dokumentation für Ihren Webanwendungsserver.

Kapitel 3. Verbindungen zu gehosteten E-Mail-Services

Um den Zugriff auf die von IBM bereitgestellten gehosteten E-Mail-Services zu ermöglichen, müssen Sie eine Verbindung zwischen der lokalen IBM EMM-Installation und IBM EMM Hosted Services konfigurieren.

Marketiers greifen auf eMessage-Funktionen über die Campaign-Benutzeroberfläche zu. Das Arbeiten mit eMessage erfordert den Aufbau einer sicheren automatischen Internetverbindung, über die Campaign E-Mail-Empfängerlisten auf IBM EMM Hosted Services hochladen kann. Mit Campaign installierte eMessage-Komponenten verwenden diese Verbindung ebenfalls, um Kontakt- und Antwortdaten in die eMessage-Systemtabellen im Campaign-Schema herunterzuladen.

Anmerkung: Jede Instanz von Campaign erfordert eine eindeutige Verbindung zu IBM EMM Hosted Services. Wenn die Campaign-Installation mehrere Partitionen enthält, erfordert jede Partition ein separates gehostetes E-Mail-Konto. Die Konten können die IP-Verbindung zu IBM EMM Hosted Services gemeinsam nutzen.

Die gesamte Kommunikation zwischen IBM EMM und IBM EMM Hosted Services erfolgt über SSL. Jede Kommunikation von IBM EMM Hosted Services ist eine Antwort auf eine Anforderung aus der lokalen Umgebung. IBM EMM Hosted Services versucht nie, eine Verbindung zu Ihrem Unternehmensnetz zu initiieren. Die gesamte Kommunikation mit IBM EMM Hosted Services geht von hinter der Unternehmensfirewall aus.

Anforderungen für die Konfiguration einer Verbindung zu IBM EMM Hosted Services

Die Konfiguration einer Verbindung zu IBM EMM Hosted Services erfordert Administratorberechtigungen und Informationen zu dem gehosteten E-Mail-Konto, das für Ihre Organisation eingerichtet ist.

Zum Konfigurieren einer gehosteten E-Mail-Verbindung benötigen Sie Folgendes:

- Benutzername und Kennwort für das gehostete E-Mail-Konto (bereitgestellt durch IBM)
- Berechtigungen zum Erstellen oder Ändern von Systembenutzern in der IBM Marketing Platform
- Administratorzugang zu Konfigurationseigenschaften, die in der lokalen IBM Marketing Platform-Installation verwaltet werden
- Administratorzugang zum Webanwendungsserver, auf dem die IBM Marketing Platform und Campaign implementiert sind

Sie müssen die Anforderungen an die Datensicherheit in Ihrem Unternehmen kennen oder jemanden konsultieren können, der die Anforderungen kennt. Bevor Sie beginnen, machen Sie sich mit diesen Prozeduren vertraut, damit Sie die erforderliche Verbindung in Übereinstimmung mit den durch Ihre Unternehmensfirewall festgelegten Einschränkungen erstellen können.

Sie müssen wissen, wie Sie vertrauenswürdige Verbindungen auf Ihrem Webanwendungsserver (entweder IBM WebSphere oder Oracle WebLogic) konfigurieren.

© Copyright IBM Corp. 1999, 2015

Voraussetzungen für den Upload von Daten in IBM EMM Hosted Services

Eine eMessage-Komponente mit dem Namen Recipient List Uploader (RLU) ist Teil Ihrer IBM Campaign-Installation. Das RLU verwendet FTP im passiven Modus, um den Upload von E-Mail-Mailing-Listen und zugehörigen Metadaten auf IBM EMM Hosted Services zu verwalten.

eMessage verwendet passives FTP zum Hochladen von Daten. Wenn passives FTP verwendet wird, agiert das RLU als lokaler Client und initiiert alle Upload-Verbindungsanforderungen. IBM EMM Hosted Services initiiert nie eine Verbindungsanforderung an Ihr Netz.

eMessage unterstützt zwei passive FTP-Methoden, explizites FTP und implizites FTP. Explizites FTP ist die Standardmethode zum Hochladen von Empfängerlisten. Wenn Sie implizites FTP verwenden möchten, müssen Sie Änderungen an den eMessage-Konfigurationseigenschaften vornehmen.

Weitere Informationen zu FTP im passiven Modus und zur Verwendung von FTP über SSL finden Sie in RFC959 und RFC2228.

Zugehörige Konzepte:

„Standard-Uploadverbindung über explizites FTP" auf Seite 13

„Daten mit implizitem FTP hochladen" auf Seite 14

Verbindungs- und Portanforderungen

Um mit IBM EMM Hosted Services zu kommunizieren, müssen Sie eine Verbindung zum Internet haben. IBM EMM Hosted Services verwendet bestimmte Ports.

Die lokale IBM EMM-Installation und IBM EMM Hosted Services verwenden die folgenden Ports für die Kommunikation.

HTTPS: Port 443

FTP-Befehlsport:

- Explizites FTP: Port 21
- Implizites FTP: Port 990

FTP-Ports für Datenupload

- Rechenzentrum in USA
  Explizites FTP: Ports 15393 bis 15424
  Implizites FTP: Ports 15600 bis 15701
- Rechenzentrum in Großbritannien
  Explizites FTP: Ports 15393 bis 15443
  Implizites FTP: Ports 15600 bis 15650

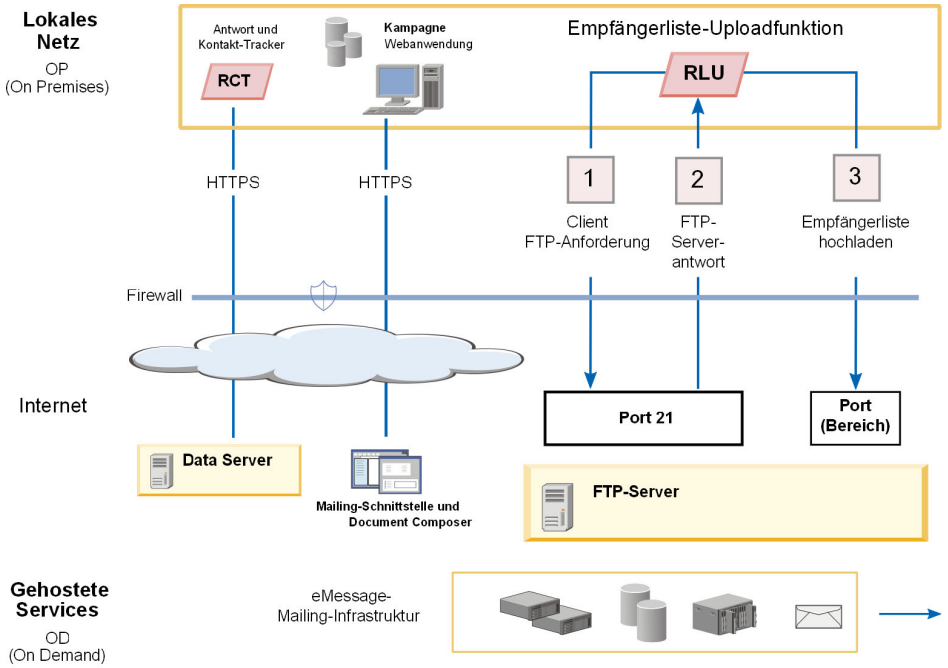
IBM EMM Hosted Services initiiert nie eine Verbindung zu Ihrem lokalen Netz. Es antwortet nur auf Verbindungsanforderungen, die von hinter Ihrer Firewall initiiert wurden.

Standard-Uploadverbindung über explizites FTP

Standardmäßig verwendet das Hochladeprogramm für die Empfängerliste (Recipient List Uploader, RLU) explizites FTP, wenn eine E-Mail-Empfängerliste vom System hochgeladen wird. Die Empfängerliste wird auch als Ausgabelistentabelle (OLT) bezeichnet.

Das RLU baut über den FTP-Standardbefehlsport (Port 21) eine Verbindung zu IBM EMM Hosted Services auf. Dann gibt es eine Anforderung aus, dass die Sitzung über SSL verschlüsselt werden soll. Das RLU handelt mit dem FTP-Server eine separate SSL-Verbindung über einen vom RLU zufällig ausgewählten Port aus. Weitere Informationen zu explizitem FTP finden Sie im RFC 2228.

Das folgende Diagramm zeigt die Standardmethode zum Hochladen von Empfängerdaten aus Campaign auf IBM EMM Hosted Services.



In der nachfolgenden Tabelle wird die Verbindungssequenz beschrieben.

Schritt	Aktion	Beschreibung
1	Anfängliche FTP-Verbindungsanforderung durch Client	Von hinter der Unternehmensfirewall initiiert das RLU eine Datenupload-Sitzung mittels FTP über explizites SSL. Das RLU sendet die SSL-Verbindungsanforderung an die Adresse für IBM EMM Hosted Services. Diese Adresse müssen Sie im Vorfeld konfigurieren. Um die Sitzung zu starten, öffnet das RLU einen zufällig ausgewählten Port auf der Clientseite als seinen FTP-Befehlsport. IBM EMM Hosted Services akzeptiert FTP-Befehlsverbindungen auf Port 21.
2	Antwort des fernen FTP-Servers	Als Antwort auf die Anforderung des RLU einer sicheren SSL-Sitzung gibt der FTP-Server den FTP-Datenport an, über den die Empfängerliste hochgeladen werden soll.

Schritt	Aktion	Beschreibung
3	Hochladen der Empfängerliste	Das RLU beginnt mit dem Hochladen der Liste auf dem angegebenen Datenport. Wenn das Hochladen abgeschlossen ist, schließt das RLU die FTP-Verbindung.

Informationen zum Datenportbereich, den der FTP-Server angeben kann, finden Sie unter „Verbindungs- und Portanforderungen" auf Seite 12.

Zugehörige Konzepte:

„Voraussetzungen für den Upload von Daten in IBM EMM Hosted Services" auf Seite 12

Zugehörige Tasks:

„Adressen zum Herstellen einer Verbindung zu IBM EMM Hosted Services konfigurieren" auf Seite 25

„Systembenutzer mit Zugriff auf IBM EMM Hosted Services konfigurieren" auf Seite 24

Verbindung für explizites FTP konfigurieren

Es ist keine zusätzliche Konfiguration erforderlich. Das RLU verwendet standardmäßig explizites FTP.

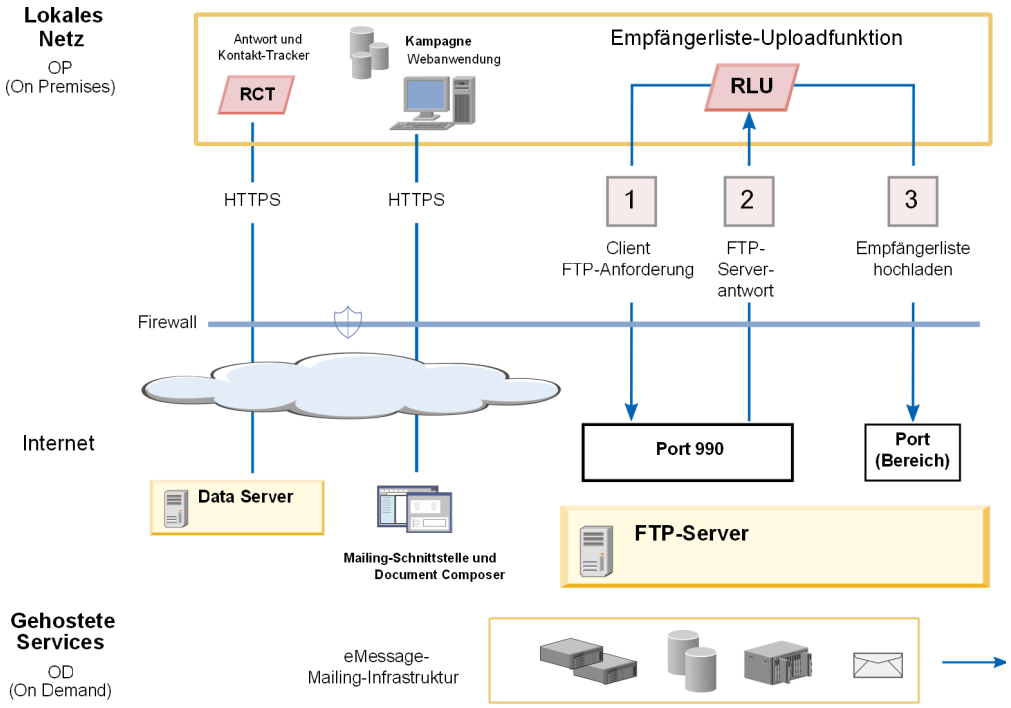
Daten mit implizitem FTP hochladen

Sie können das RLU dafür konfigurieren, zum Hochladen von E-Mail-Empfängerlisten implizites FTP zu verwenden. Implizites FTP verwendet Port 990, um eine Verbindung zu IBM EMM Hosted Services herzustellen.

Wenn Sie das RLU für implizites FTP aktivieren, wird die gesamte Sitzung von Anfang an verschlüsselt. Im Gegensatz zu implizitem FTP fordert das RLU bei einer Verbindung über explizites FTP eine sichere Leitung an.

Um implizites FTP zum Hochladen von Empfängerlisten zu verwenden, müssen Sie eine Systemkonfigurationseigenschaft in den eMessage-Konfigurationseigenschaften anzeigen und konfigurieren.

Das folgende Diagramm zeigt, wie das RLU Empfängerdaten auf IBM EMM Hosted Services hochlädt, wenn das System dafür konfiguriert ist, implizites FTP zu verwenden.



In der nachfolgenden Tabelle wird die Verbindungssequenz beschrieben.

Schritt	Aktion	Beschreibung
1	Anfängliche FTP-Verbindungsanforderung durch Client	Von hinter der Unternehmensfirewall initiiert das RLU eine Datenupload-Sitzung mittels FTP über SSL. Das RLU sendet die SSL-Verbindungsanforderung an die Adresse für IBM EMM Hosted Services. Diese Adresse müssen Sie im Vorfeld konfigurieren. Um die Sitzung zu starten, öffnet das RLU Port 990. IBM EMM Hosted Services akzeptiert verschlüsselte FTP-Befehlsverbindungen nur auf Port 990.
2	Antwort des fernen FTP-Servers	Wenn IBM EMM Hosted Services die Anforderung als gültige implizite FTP-Anforderung erkennt, akzeptiert der FTP-Server die Verbindungsanforderung und gibt den FTP-Datenport an, über den die Empfängerliste hochgeladen werden soll. Informationen zum Datenportbereich, den der FTP-Server angeben kann, finden Sie unter „Verbindungs- und Portanforderungen" auf Seite 12.
3	Hochladen der Empfängerliste	Das RLU beginnt mit dem Hochladen der Liste auf dem angegebenen Datenport. Wenn das Hochladen abgeschlossen ist, schließt das RLU die FTP-Verbindung.

Zugehörige Konzepte:

„Voraussetzungen für den Upload von Daten in IBM EMM Hosted Services" auf Seite 12

Zugriff auf die Konfigurationsparameter zum Hochladen von Daten mit implizitem FTP

Um das System für die Verwendung von implizitem FTP zum Hochladen zu konfigurieren, müssen Sie Konfigurationseigenschaften konfigurieren, die standardmäßig ausgeblendet sind. Diese Eigenschaften werden durch Ausführung eines Scripts sichtbar gemacht.

Informationen zu diesem Vorgang

Damit das System für die Verwendung von implizitem FTP zum Hochladen von Daten konfiguriert werden kann, müssen Sie die folgenden Konfigurationseigenschaften einblenden. Diese Eigenschaften sind standardmäßig ausgeblendet.

- `eMessage > serverComponentsAndLocations > hostedServices > ftpPort`
- `eMessage > serverComponentsAndLocations > hostedServices > useFTPImplicitSSL`

Mit dieser Prozedur werden die Konfigurationseigenschaften angezeigt, aber nicht konfiguriert. Um implizites FTP zu aktivieren, müssen Sie in der eMessage-Konfiguration auf diese Eigenschaften zugreifen und sie konfigurieren. Informationen zum Konfigurieren dieser Eigenschaften finden Sie im Abschnitt „Hochladen über implizites FTP aktivieren” auf Seite 17.

Vorgehensweise

Um die Eigenschaften `ftpPort` und `useFTPImplicitSSL` einzublenden, müssen Sie das Script `switch_config_visibility` im Verzeichnis **tools** über das Befehlszeilenscript ausführen.

Windows

```
\switch_config_visibility.bat -p
"Affinium|eMessage|serverComponentsAndLocations|hostedServices|ftpPort" -v
true
\switch_config_visibility.bat -p
"Affinium|eMessage|serverComponentsAndLocations|hostedServices|
useFTPImplicitSSL" -v true
```

UNIX

```
/switch_config_visibility.sh
"Affinium|eMessage|serverComponentsAndLocations|hostedServices|ftpPort" -v
true
/switch_config_visibility.sh
"Affinium|eMessage|serverComponentsAndLocations|hostedServices|
useFTPImplicitSSL" -v true
```

Nächste Schritte

Sie müssen den Webanwendungsserver erneut starten, um diese Eigenschaften in der eMessage-Konfiguration anzuzeigen.

Zugehörige Tasks:

„Zugriff auf zusätzliches Protokoll der Mailing-Ausführung konfigurieren” auf Seite 46

Hochladen über implizites FTP aktivieren

Um implizites FTP zu aktivieren, müssen Sie die eMessage-Konfiguration aktualisieren.

Vorbereitende Schritte

Zum Ausführen dieser Aufgabe müssen Sie zwei Konfigurationseigenschaften anzeigen. Weitere Informationen finden Sie unter „Zugriff auf die Konfigurationsparameter zum Hochladen von Daten mit implizitem FTP" auf Seite 16.

Vorgehensweise

1. Navigieren Sie zu `Einstellungen > Konfiguration > eMessage > serverComponentsAndLocations > hostedServices`.
2. Klicken Sie auf **Einstellungen bearbeiten**.
   - Vergewissern Sie sich, dass `useFTPImplicitSSL` auf `true` festgelegt ist.
   - Legen Sie `ftpPort` auf `990` fest.
3. Speichern Sie Ihre Änderungen.

Nächste Schritte

Die Änderungen werden erst wirksam, nachdem Sie den Webanwendungsserver und den Campaign-Listener erneut gestartet haben. Sie können dies jetzt durchführen oder warten, bis Sie alle Startkonfigurationsschritte abgeschlossen haben.

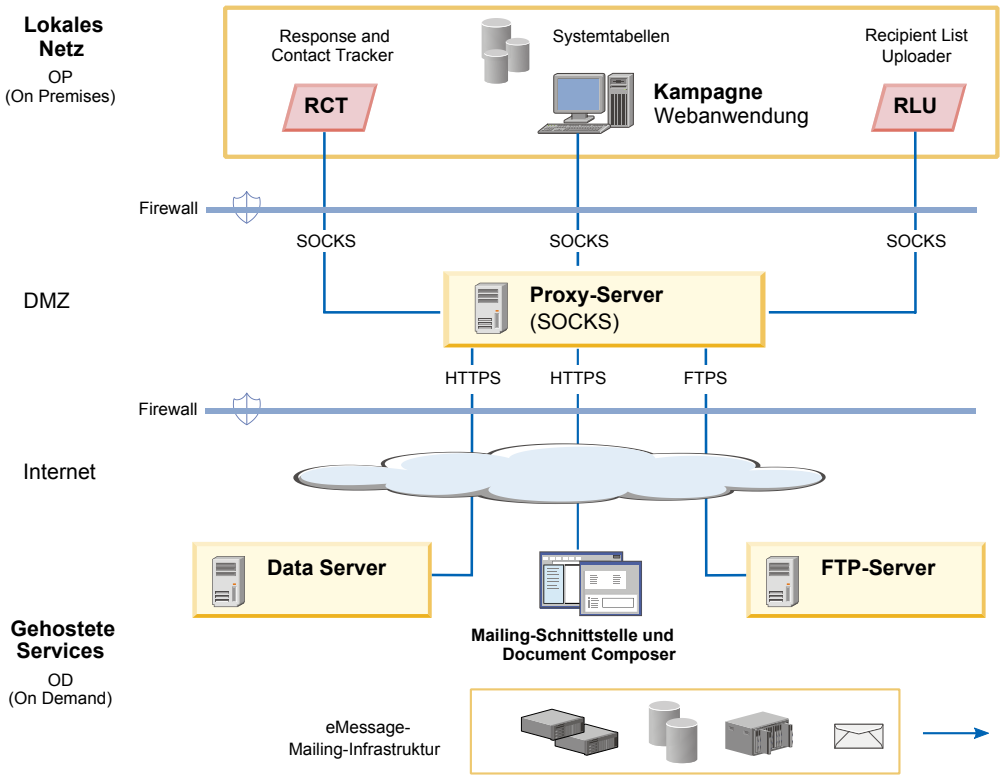
Verbindungsaufbau über einen HTTP-Proxy

Wenn die Firewallregeln Ihres Unternehmens keine direkte Kommunikation mit dem öffentlichen Internet zulassen, können Sie über einen HTTP-Proxy-Server eine Verbindung zu IBM EMM Hosted Services herstellen. eMessage unterstützt den Verbindungsaufbau über einen SOCKS-Proxy-Server, der HTTPS- und FTPS-Datenverkehr zulässt.

eMessage unterstützt SOCKS Protokollversion 5.

Anmerkung: Wenn Sie die Verbindung zu IBM EMM Hosted Services über einen Proxy-Server herstellen möchten, müssen Sie Campaign Version 8.5.0.1 oder höher installieren.

Das nachfolgende Diagramm zeigt die Kommunikation zwischen der lokalen und gehosteten Umgebungen, wenn Sie einen SOCKS-Proxy verwenden.



Sie konfigurieren den SOCKS-Proxy-Server in der lokalen On-Premises-Umgebung. Stellen Sie vor Beginn der Konfiguration des Proxy-Servers sicher, dass folgende Voraussetzungen erfüllt sind:

- Der Proxy-Server muss ein SOCKS-Proxy-Server sein.
- Der Proxy-Server muss auf die OP-Umgebung von eMessage zugreifen können. Der Server muss den Datenverkehr sowohl zu den Ports, die für das Rechenzentrum konfiguriert wurden, das von Ihrem gehosteten E-Mail-Konto verwendet wird, als auch den Datenverkehr von diesen Ports unterstützen. IBM verwaltet Rechenzentren in den USA und Großbritannien.
- Die OP-Umgebung von eMessage muss auf den SOCKS-Proxy-Server zugreifen können.

Routing für FTPS- und HTTPS-Datenverkehr über einen SOCKS-Proxy konfigurieren

Um über einen SOCKS-Proxy auf die gehosteten E-Mail-Ressourcen zuzugreifen, müssen Sie den Webanwendungsserver an der Position aktualisieren, an der Sie IBM Campaign implementiert haben. Zudem müssen Sie die Startscripts für das RCT und die RLU von eMessage ändern.

Vorgehensweise

- Wenden Sie für FTPS-Verkehr die folgenden Konfigurationen für den RLU und den Webanwendungsserver an:

Einstellung	Beschreibung
`-Dibm.unica.emessage.ftps.proxy.host = <socksHost>`	Hostname oder IP des SOCKS-Proxy.

Einstellung	Beschreibung
-Dibm.unica.emessage.ftps.proxy.port = <socksPort>	Der Port, auf dem der SOCKS-Proxy aktiv ist.
-Dibm.unica.emessage.ftps.proxy.match.hosts= <durch Kommas getrennte Liste mit Hostnamen und IP-Adressen>	Hostnamen und IP-Adressen, die beim Weiterleiten von Datenverkehr über den SOCKS-Proxy verwendet werden. Geben Sie die Werte für das von Ihrem Konto verwendete Rechenzentrum an.

Wenn die lokalen und gehosteten Umgebungen eine Datenverbindung herstellen, ist die für -Dibm.unica.emessage.ftps.proxy.match.hosts angegebene IP-Adresse diejenige, die der ferne FTP-Server an den lokalen FTP-Client sendet.

Setzen Sie -Dibm.unica.emessage.ftps.proxy.match.hosts auf einen der nachfolgend genannten Werte. Der Wert, den Sie eingeben, richtet sich nach dem Rechenzentrum, das von Ihrem gehosteten E-Mail-Konto verwendet wird.

Hostname und IP-Adressen für das Rechenzentrum in den USA:

```
-Dibm.unica.emessage.ftps.proxy.match.hosts=

ftp-
em.unicaondemand.com,192.86.44.132,192.86.44.133,192.86.44.134,192.86.45.132,192.86.45.133,192.86.45.134
```

Hostname und IP-Adressen für das Rechenzentrum in Großbritannien:

```
-Dibm.unica.emessage.ftps.proxy.match.hosts=

ftp-em-
eu.unicaondemand.com,192.86.45.132,192.86.45.133,192.86.45.134,192.86.44.132,192.86.44.133,192.86.44.134
```

- Wenden Sie für HTTPS-Verkehr die folgenden Konfigurationen für den RCT und den Webanwendungsserver an:

Einstellung	Beschreibung
-Dibm.unica.emessage.https.proxy.host=<socksHost>	Hostname oder IP des SOCKS-Proxy
-Dibm.unica.emessage.https.proxy.port=<socksPort>	Der Port, auf dem der SOCKS-Proxy aktiv ist
-Dibm.unica.emessage.https.proxy.type=SOCKS	Der Proxy-Servertyp. Sie müssen einen SOCKS-Proxy-Server verwenden.

Authentifizierung für den Zugriff auf einen SOCKS-Proxy konfigurieren

Wenn der SOCKS-Proxy eine Authentifizierung erfordert, müssen Sie den Webanwendungsserver, das RLU und den RCT für die Bereitstellung der Zugriffsberechtigungsnachweise konfigurieren.

Vorgehensweise

Konfigurieren Sie Folgendes für den Webanwendungsserver, das RLU und den RCT. Die Werte für Benutzername und Kennwort müssen den Berechtigungsnachweisen entsprechen, die zur Authentifizierung am Proxy erforderlich sind.

```
-Dibm.unica.emessage.proxy.auth.user = <Benutzername>
-Dibm.unica.emessage.proxy.auth.password = <Kennwort>
```

Den RCT zur Verwendung eines SOCKS-Proxy konfigurieren

Ändern Sie den RCT, damit er über einen SOCKS-Proxy-Server kommuniziert. Die erforderlichen Änderungen richten sich nach dem verwendeten Betriebssystem.

Vorgehensweise

- Für den RCT in Windows-Umgebungen müssen der Datei `common.bat` die folgenden Proxy-Argumente hinzugefügt werden. Die Datei `common.bat` befindet sich im Verzeichnis `//eMessage/bin` Ihrer lokalen eMessage-Installation.

```
set RCT_PROXY_ARGS=

-Dibm.unica.emessage.https.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.https.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.https.proxy.type=SOCKS

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>

set RCT_JAVA_ARGS=%BASE_VM_ARGS% %RCT_MEM_ARGS%

%RCT_EXTRA_VM_ARGS% %RCT_PROXY_ARGS%
```

- Für den RCT in UNIX-Umgebungen müssen der Datei `common.sh` die folgenden Proxy-Argumente hinzugefügt werden. Die Datei `common.sh` befindet sich im Verzeichnis `\\eMessage\bin` Ihrer lokalen eMessage-Installation.

  Anmerkung: Die Dateien `rlu.sh`, `rct.sh` und `setenv.sh` dürfen nicht direkt geändert werden. Änderungen werden vom System überschrieben.

```
RCT_PROXY_ARGS="

-Dibm.unica.emessage.https.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.https.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.https.proxy.type=SOCKS

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>"

RCT_JAVA_ARGS="${BASE_VM_ARGS} ${RCT_MEM_ARGS} ${RCT_EXTRA_VM_ARGS}
${RCT_PROXY_ARGS}"
```

Das RLU zur Verwendung eines SOCKS-Proxy konfigurieren

Ändern Sie das RLU, damit es über einen SOCKS-Proxy-Server kommuniziert. Die erforderlichen Änderungen richten sich nach dem verwendeten Betriebssystem.

Vorgehensweise

- Für den RLU in Windows-Umgebungen müssen der Datei `common.bat` die folgenden Proxy-Argumente hinzugefügt werden. Die Datei `common.bat` befindet sich im Verzeichnis `//eMessage/bin` Ihrer lokalen eMessage-Installation.

```
set RLU_PROXY_ARGS=

-Dibm.unica.emessage.ftps.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.ftps.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.ftps.proxy.match.hosts=<durch Kommas getrennte Liste mit
Hostnamen und IP-Adressen>

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>

set RLU_JAVA_ARGS=%BASE_VM_ARGS% %RLU_MEM_ARGS% %RLU_EXTRA_VM_ARGS%

%RLU_PROXY_ARGS%
```

- Für den RLU in UNIX-Umgebungen müssen der Datei `common.sh` die folgenden Proxy-Argumente hinzugefügt werden. Die Datei `common.sh` befindet sich im Verzeichnis `\\eMessage\bin` Ihrer lokalen eMessage-Installation.

  Anmerkung: Die Dateien `rlu.sh`, `rct.sh` und `setenv.sh` dürfen nicht direkt geändert werden. Änderungen werden vom System überschrieben.

```
RLU_PROXY_ARGS="

-Dibm.unica.emessage.ftps.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.ftps.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.ftps.proxy.match.hosts=<durch Kommas getrennte Liste mit
Hostnamen und IP-Adressen>

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>"

RLU_JAVA_ARGS="${BASE_JAVA_ARGS} ${RLU_MEM_ARGS} ${RLU_EXTRA_VM_ARGS}

${RLU_PROXY_ARGS}"
```

Webanwendungsserver zur Verwendung eines SOCKS-Proxy konfigurieren

Um über einen Proxy-Server eine Verbindung zu IBM EMM Hosted Services herzustellen, müssen Sie die Konfiguration des Webanwendungsservers ändern. Ändern Sie für IBM WebSphere-Server die allgemeinen JVM-Argumente. Für Oracle Weblogic-Server ändern Sie das Script `SetDomainEnv`.

Vorgehensweise

- Wenn Sie IBM WebSphere als Webanwendungsserver verwenden, fügen Sie den allgemeinen JVM-Argumenten von WebSphere folgende Argumente hinzu:

```
-Dibm.unica.emessage.https.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.https.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.https.proxy.type=SOCKS

-Dibm.unica.emessage.ftps.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.ftps.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.ftps.proxy.match.hosts=<durch Kommas getrennte Liste mit
Hostnamen und IP-Adressen>

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>
```

- Wenn Sie Oracle Weblogic als Webanwendungsserver verwenden, ändern Sie das Script `setDomainEnv`. Die erforderlichen Änderungen richten sich nach dem verwendeten Betriebssystem.

  Nehmen Sie in Windows-Umgebungen folgende Änderungen vor:

```
JAVA_OPTIONS =%{JAVA_OPTIONS}

-Dibm.unica.emessage.https.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.https.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.https.proxy.type=SOCKS

-Dibm.unica.emessage.ftps.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.ftps.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.ftps.proxy.match.hosts=<durch Kommas getrennte Liste mit
Hostnamen und IP-Adressen>

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>
```

  Nehmen Sie in UNIX-Umgebungen folgende Änderungen vor:

```
JAVA_OPTIONS ='${JAVA_OPTIONS}

-Dibm.unica.emessage.https.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.https.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.https.proxy.type=SOCKS

-Dibm.unica.emessage.ftps.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.ftps.proxy.port=<POXY_PORT>

-Dibm.unica.emessage.ftps.proxy.match.hosts=<durch Kommas getrennte Liste mit
Hostnamen und IP-Adressen>

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>'
```

Downloadrate für Daten und Porteinstellung

Eine eMessage-Komponente namens Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) wird als Teil Ihrer IBM Campaign-Installation installiert. Der RCT fordert regelmäßig E-Mail-Antwort- und -Verfolgungsdaten von IBM EMM Hosted Services an. Standardmäßig gibt der RCT alle fünf Sekunden eine Datenanforderung aus.

Der RCT gibt Datenanforderungen über HTTPS (HTTP über SSL) aus. IBM EMM Hosted Services akzeptiert HTTPS-Verbindungsanforderungen an Port 443, jedoch nur von Hosts, die beim Startprozess des gehosteten E-Mail-Kontos angegeben wurden.

Zugehörige Konzepte:

Kapitel 4, „RCT (Response and Contact Tracker)", auf Seite 35

Anforderung für den Systembenutzer für den Zugriff auf IBM EMM Hosted Services

eMessage-Komponenten müssen auf die IBM EMM Hosted Services zugreifen können, ohne dass die manuelle Eingabe von Berechtigungsnachweisen für die Anmeldung erforderlich ist. Um die automatische Anmeldung einzurichten, definieren Sie einen Systembenutzer in Marketing Platform, der die erforderlichen Zugriffsberechtigungen bereitstellen kann.

Um die Benutzeradministration und Fehlersuche zu vereinfachen, können Sie einen vorhandenen Systembenutzer ändern, damit dieser auf gehostete Services und lokale Systemtabellen zugreifen kann. Sie können einen einzelnen Systembenutzer konfigurieren, um Berechtigungsnachweise für mehrere Systeme bereitzustellen. Beispielsweise können Sie durch Ändern der Konfiguration des Campaign-Systembenutzers einen einzelnen Benutzer erstellen, der automatisch auf IBM EMM Hosted Services und die eMessage-Systemtabellen im Campaign-Schema zugreifen kann.

Die erforderlichen Berechtigungsnachweise für den Zugriff auf IBM EMM Hosted Services sind der Benutzername und das Kennwort, die IBM für Ihren gehosteten Messaging-Account bereitgestellt hat. Welche Berechtigungsnachweise Sie verwenden, hängt davon ab, ob Sie die Verbindung zu dem von IBM in den USA oder in Großbritannien betriebenen Rechenzentrum herstellen. Fragen Sie bei IBM nach, welches Rechenzentrum Sie verwenden sollen.

Spezielle Informationen zum Konfigurieren eines Systembenutzers für die Kommunikation mit IBM EMM Hosted Services finden Sie im *IBM eMessage Einstiegs- und Administratorhandbuch*.

Allgemeine Informationen zum Erstellen von Systembenutzern und Datenquellen finden Sie im *IBM Marketing Platform-Administratorhandbuch*.

Anforderung für den Partitionszugriff für IBM EMM Hosted Services

IBM eMessage-Komponenten in der Partition müssen befugt sein, automatisch gültige Berechtigungsnachweise für die Anmeldung bereitzustellen, wenn versucht wird, mit IBM EMM Hosted Services zu kommunizieren. Zu diesem Zweck müs-

sen Sie die Berechtigungsnachweise für die Anmeldung für IBM EMM Hosted Services einem Marketing Platform-Benutzer hinzufügen. Dieser Benutzer wird zum eMessage-Systembenutzer.

Sie können die Plattform-Datenquelle mit den IBM EMM Hosted Services-Berechtigungsnachweisen zum eMessage-Systembenutzer hinzufügen. Bei diesem Benutzer kann es sich um denselben Systembenutzer handeln, der auf die Campaign-Systemtabellen in der Partition zugreift.

Die Schritte für die Konfiguration von Systembenutzern für eine Partition sind identisch mit denen, die bei der eMessage-Erstinstallation durchgeführt werden, bei der die erste Partition erstellt wurde. Weitere Informationen zum Hinzufügen von Berechtigungsnachweisen für die Anmeldung für IBM EMM Hosted Services zu einem Systembenutzer finden Sie im *IBM eMessage-Einstiegs- und Administratorhandbuch*.

Die erforderlichen Berechtigungsnachweise für den Zugriff auf IBM EMM Hosted Services sind der Benutzername und das Kennwort, die IBM während des ersten Startprozesses bereitgestellt hat.

Wichtig: Für jede zusätzliche Partition müssen Sie einen eigenen Benutzernamen und ein eigenes Kennwort von IBM anfordern.

Systembenutzer mit Zugriff auf IBM EMM Hosted Services konfigurieren

Die eMessage-Komponenten in Campaign müssen in der Lage sein, ohne Aufforderung zur Eingabe von Anmeldedaten auf IBM EMM Hosted Services zuzugreifen. Die in IBM Marketing Platform konfigurierten Systembenutzer können eine Datenquelle referenzieren, die die erforderlichen Angaben zu Benutzername und Kennwort bereitstellt. Sie können die Datenquelle einem neuen Systembenutzer oder einem vorhandenen Systembenutzer hinzufügen. Zur Vereinfachung der Benutzerverwaltung können Sie einen bereits für den Zugriff auf das Campaign-Schema konfigurierten Systembenutzer aktualisieren, damit er auch auf IBM EMM Hosted Services zugreifen kann.

Vorbereitende Schritte

Damit Sie diese Aufgabe ausführen können, müssen Sie den Benutzernamen und das Kennwort für IBM EMM Hosted Services kennen, die IBM Ihrem gehosteten E-Mail-Konto zugewiesen hat. Der Erhalt des Benutzernamens und Kennworts ist Teil des Konto-Startprozesses.

Sie müssen über die entsprechenden Zugriffsberechtigungen verfügen und die Vorgehensweise zum Erstellen von Systembenutzern und Datenquellen in der IBM Marketing Platform kennen.

Informationen zu diesem Vorgang

Anmerkung: Wenn Ihre Installation mehrere Partitionen enthält, müssen Sie diese Aufgabe für jede Partition ausführen. Systembenutzer können nicht partitionsübergreifend gemeinsam genutzt werden.

Vorgehensweise

1. Erstellen Sie eine Plattformdatenquelle, die den Benutzernamen und das Kennwort enthalten soll, die für den Zugriff auf IBM EMM Hosted Services benötigt

werden. Um optimale Ergebnisse zu erzielen und die Verwaltung zu vereinfachen, geben Sie dieser Datenquelle den Namen UNICA_HOSTED_SERVICES. Konfigurieren Sie diese Datenquelle wie folgt.

Geben Sie unter **Data Source Login** (Datenquellenanmeldung) den Benutzernamen ein, den Sie während des Konto-Startprozesses von IBM erhalten haben.

Geben Sie unter **Data Source Password** (Datenquellenkennwort) das Kennwort ein, das Sie während des Konto-Startprozesses von IBM erhalten haben.

2. Geben Sie die Datenquelle in der eMessage-Konfiguration an. Verwenden Sie die Konfigurationseigenschaft **amDataSourceForAcctCredentials**.

   Sie finden die Konfigurationseigenschaft in `eMessage > partitions > partition[n] > hostedAccountInfo > amDataSourceForAcctCredentials`.

   Standardmäßig ist die Datenquelle `UNICA_HOSTED_SERVICES` angegeben.

3. Geben Sie einen Systembenutzer für den Zugriff auf IBM EMM Hosted Services an. Sie können einen bereits vorhandenen Benutzer angeben oder einen Benutzer erstellen. Verwenden Sie in der eMessage-Konfiguration die Konfigurationseigenschaft **amUserForAcctCredentials**.

   Sie finden die Konfigurationseigenschaft in `eMessage > partitions > partition[n] > hostedAccountInfo > amUserForAcctCredentials`.

   Standardmäßig ist der Benutzer `asm_admin` angegeben.

4. Fügen Sie dem in Schritt 3 angegebenen Systembenutzer die Datenquelle hinzu, die in Schritt 1 konfiguriert wurde.

Nächste Schritte

Sie müssen den Webanwendungsserver erneut starten, damit die Konfigurationsänderungen wirksam werden.

Zugehörige Konzepte:

„Standard-Uploadverbindung über explizites FTP" auf Seite 13

„Prüfung der Systemkonfigurationen" auf Seite 39

Konfigurieren der Adressen zur Verbindungsherstellung mit IBM EMM Hosted Services

Um eine korrekte Verbindung zu IBM EMM Hosted Services zu gewährleisten, müssen Sie die Adressen als Werte für Konfigurationseigenschaften in die eMessage-Konfiguration eingeben. Welche Verbindungsadresse Sie eingeben, hängt davon ab, ob Sie eine Verbindung zum IBM Rechenzentrum in den USA oder zum IBM Rechenzentrum in Großbritannien herstellen.

Fragen Sie bei IBM nach, welches Rechenzentrum von Ihrem gehosteten E-Mail-Konto genutzt wird.

Weitere Informationen zum Konfigurieren von Verbindungsinformationen finden Sie unter „Adressen zum Herstellen einer Verbindung zu IBM EMM Hosted Services konfigurieren".

Adressen zum Herstellen einer Verbindung zu IBM EMM Hosted Services konfigurieren

Um eine korrekte Verbindung zu IBM EMM Hosted Services zu gewährleisten, müssen Sie die Adressen als Werte für Konfigurationseigenschaften in die eMes-

sage-Konfiguration eingeben. Welche Verbindungsadresse Sie eingeben, hängt davon ab, ob Sie eine Verbindung zum IBM Rechenzentrum in den USA oder zum IBM Rechenzentrum in Großbritannien herstellen.

Vorbereitende Schritte

Fragen Sie bei IBM nach, welches Rechenzentrum von Ihrem gehosteten E-Mail-Konto genutzt wird.

Vorgehensweise

Navigieren Sie in IBM Marketing Platform zu **Einstellungen > Konfiguration**. Navigieren Sie in der eMessage-Konfiguration zu den folgenden eMessage-Konfigurationseigenschaften und bestätigen oder aktualisieren Sie die Verbindungseinstellungen, je nachdem, welches Rechenzentrum Ihr Konto verwendet.
Wenn Ihr Konto eine Verbindung zum Rechenzentrum in den USA herstellt, übernehmen Sie die Standardeinstellungen.

- `eMessage > serverComponentsAndLocations > hostedServices> uiHostName`

  Die Standardeinstellung ist `em.unicaondemand.com`.

  Soll eine Verbindung zum IBM Rechenzentrum in Großbritannien hergestellt werden, ändern Sie diesen Wert in

  `em-eu.unicaondemand.com`.
- `eMessage > serverComponentsAndLocations > hostedServices> dataHostName`

  Die Standardeinstellung ist `em.unicaondemand.com`.

  Soll eine Verbindung zum IBM Rechenzentrum in Großbritannien hergestellt werden, ändern Sie diesen Wert in

  `em-eu.unicaondemand.com`.
- `eMessage > serverComponentsAndLocations > hostedServices> ftpHostName`

  Die Standardeinstellung ist `ftp-em.unicaondemand.com`.

  Soll eine Verbindung zum IBM Rechenzentrum in Großbritannien hergestellt werden, ändern Sie diesen Wert in

  `ftp-em-eu.unicaondemand.com`.

Nächste Schritte

Wenn Sie eine Konfigurationseigenschaft ändern, müssen Sie den Webanwendungsserver erneut starten, um die Änderungen zu übernehmen.

Zugehörige Konzepte:

„Standard-Uploadverbindung über explizites FTP" auf Seite 13

Konfigurieren der sicheren Kommunikation für gehostete E-Mail

Kommunikationsverbindungen zwischen dem E-Mail-Marketer und IBM EMM Hosted Services erfolgen über Secure Sockets Layer (SSL). Sie müssen die Konfiguration des Webanwendungsservers ändern, um SSL nutzen zu können. Für die erforderlichen Änderungen benötigen Sie das Java™-Dienstprogramm `keytool`.

Die Konfiguration der sicheren Kommunikation beinhaltet die folgenden Aktionen:

- Generieren eines vertrauenswürdigen Keystores.
- Beziehen eines digitalen Zertifikats von IBM EMM Hosted Services

- Hinzufügen des vertrauenswürdigen Keystores zum Webanwendungsserver
- Importieren des digitalen Zertifikats von IBM EMM Hosted Services in den vertrauenswürdigen Keystore

Die genauen Schritte zur Konfiguration von SSL und deren Abfolge sind abhängig von dem Typ und der Version des Webanwendungsservers (WebSphere oder WebLogic), auf dem Sie IBM Marketing Platform und IBM Campaign implementiert haben.

Die Konfiguration für WebLogic finden Sie unter „Konfigurieren von SSL bei Verwendung von WebLogic" auf Seite 28.

Die Konfiguration für WebSphere finden Sie unter „Konfigurieren von SSL bei Verwendung von IBM WebSphere" auf Seite 31.

Generieren eines vertrauenswürdigen Keystores

Führen Sie die folgende Prozedur durch, um einen Identity-Keystore und einen vertrauenswürdigen Keystore zu erstellen, die Sie benötigen, wenn Sie IBM eMessage dafür konfigurieren, über SSL mit IBM EMM Hosted Services zu kommunizieren. Sie fügen die Keystores dem Webanwendungsserver hinzu, wenn Sie SSL konfigurieren.

Informationen zu diesem Vorgang

IBM verwendet die folgenden Stichprobenwerte für die in diesem Abschnitt enthaltenen Prozeduren.

- Identity-Keystore: `IBMUnicaClientIdentity.jks`
- Alias für den Identity-Keystore: `IBMUnicaClientIdentity`
- Kennwort (`-storepass`) für den Identity-Keystore: `clientPwd`
- Sicherheitsschlüssel (`-keypass`) für den Identity-Keystore: `clientPwd`
- Auf dem Identity-Keystore basierendes Zertifikat: `ClientCertificate.cer`
- Vertrauenswürdiger Keystore: `IBMUnicaTrust.jks`
- Kennwort (`-storepass`) für den vertrauenswürdigen Keystore: `trustPwd`

Die tatsächlich einzugebenden Werte müssen sich auf Ihre Installation beziehen.

Um die Schritte dieser Prozedur abzuschließen, führen Sie das Java-Dienstprogramm `keytool` aus der Befehlszeile aus.

Vorgehensweise

1. Erstellen Sie einen Identity-Keystore. Verwenden Sie den Befehl `genkey`, wie im folgenden Beispiel dargestellt.

   Bei dem Beispiel wird ein Identity-Keystore mit dem Namen `IBMUnicaClientIdentity.jks` erstellt. Sie können für den von Ihnen erstellten Identity-Keystore einen anderen Namen verwenden.

   ```
   keytool -genkey -alias IBMUnicaClientIdentity -keyalg RSA -keystore
   <IBMUnicaClientIdentity.jks> -keypass <clientPwd> -validity 1000 -dname
   "CN=hostName, O=myCompany" -storepass <clientPwd>
   ```

   Folgendes beachten:

   - Sie verwenden die Werte für `alias`, `keystore`, `keypass` und `storepass` später in dieser Prozedur und wenn Sie SSL im Webanwendungsserver konfigurieren.

- Bei WebSphere 6.0 muss das Keystore-Kennwort (`-storepass`) mit dem Schlüsselkennwort (`-keypass`) identisch sein.
- Im definierten Namen (`-dname`) ist der allgemeine Name (`CN`) mit dem für den Zugriff auf IBM EMM verwendeten Hostnamen identisch. Wenn beispielsweise die URL für IBM EMM `https://hostName.example.com:7002/unica/jsp` lautet, ist der CN `hostName.example.com`. Der CN-Teil des definierten Namens ist der einzige erforderliche Teil; Organisation (`O`) und Organisationseinheit (`OU`) sind nicht erforderlich.

2. Erstellen Sie ein Zertifikat basierend auf dem Identity-Keystore. Verwenden Sie den Befehl `export`, wie im folgenden Beispiel dargestellt.

   Bei dem Beispiel wird ein Zertifikat mit dem Namen `ClientCertificate.cer` erstellt. Sie können für das von Ihnen erstellte Zertifikat einen anderen Namen verwenden.

   Die Werte für `keystore`, `storepass` und `alias` müssen den Werten entsprechen, die Sie für den Identity-Keystore angegeben haben.

   ```
   keytool -export -keystore <IBMUnicaClientIdentity.jks> -storepass
   <clientPwd> -alias IBMUnicaClientIdentity -file <ClientCertificate.cer>
   ```

3. Generieren Sie den vertrauenswürdigen Keystore. Verwenden Sie den Befehl `import`, wie im folgenden Beispiel dargestellt.

   Bei dem Beispiel wird ein vertrauenswürdiger Keystore mit dem Namen `IBMUnicaTrust.jks` erstellt. Sie können für den von Ihnen erstellten vertrauenswürdigen Keystore einen anderen Namen verwenden.

   ```
   keytool –import -alias IBMUnicaClientIdentity -file
   <ClientCertificate.cer> -keystore <IBMUnicaTrust.jks> -storepass
   <trustPwd>
   ```

   Geben Sie **Y** ein, wenn Sie aufgefordert werden, die Vertrauenswürdigkeit des Zertifikats zu bestätigen.

Nächste Schritte

Notieren Sie sich die Werte, die Sie für die folgenden Variablen definiert haben. Ihre Werte können sich von den in dem Beispiel angegebenen Werten unterscheiden.

- `alias` (in dem Beispiel: `IBMUnicaClientIdentity`)
- `identity keystore` (in dem Beispiel: `IBMUnicaClientIdentity.jks`)
- `storepass` (in dem Beispiel: `trustPwd`) Der Wert `storepass` für den vertrauenswürdigen Keystore kann sich von dem Wert `storepass` für den Identity-Keystore und das Zertifikat unterscheiden.
- `keystore` (in dem Beispiel: `IBMUnicaTrust.jks`) Abhängig von Ihrem Webanwendungsserver geben Sie auch den Identity-Keystore an.

Sie geben diese installationsspezifischen Werte an, wenn Sie SSL auf dem Webanwendungsserver für Ihre IBM EMM-Installation konfigurieren.

Konfigurieren von SSL bei Verwendung von WebLogic

Dieser Abschnitt beschreibt die erforderlichen Schritte zum Konfigurieren von SSL, wenn Sie IBM EMM-Komponenten auf Oracle WebLogic implementieren. Diese Änderung ist erforderlich, damit eMessage-Komponenten, die in Campaign betrieben werden, über SSL mit IBM EMM Hosted Services kommunizieren können.

Informationen zu diesem Vorgang

Eine genaue Anleitung dazu, wie Sie auf der Oracle WebLogic-Benutzeroberfläche navigieren und mit dieser arbeiten, finden Sie in der Dokumentation zu der von Ihnen verwendeten Version von Oracle WebLogic.

Vorgehensweise

Führen Sie die folgenden Aufgaben aus:

- Ändern des WebLogic-Startscripts
- Ändern der WebLogic-Konfiguration
- Beziehen eines digitalen Zertifikats von IBM EMM Hosted Services
- Erstellen eines vertrauenswürdigen Keystores und Importieren des digitalen Zertifikats von IBM

WebLogic-Startscript ändern

Wenn Sie Campaign auf WebLogic implementiert haben, müssen Sie das WebLogic-Startscript und die WebLogic-Konfiguration für SSL ändern, sodass WebLogic die sichere Kommunikation zwischen lokal installierten eMessage-Komponenten und IBM EMM Hosted Services erkennt und akzeptiert.

Vorgehensweise

Fügen Sie folgende Argumente zu den JAVA_OPTIONS im WebLogic-Startscript hinzu.

- `-Dweblogic.security.SSL.allowSmallRSAExponent=true`
- WebLogic-Version 12c oder höher:
  `-Dweblogic.security.SSL.protocolVersion=TLS1`

  Alle Vorgängerversionen: `-Dweblogic.security.SSL.nojce=true`

WebLogic-Konfiguration ändern

Sie müssen die SSL-Konfiguration in WebLogic ändern.

Vorgehensweise

Nehmen Sie über die WebLogic-Konsole die folgende Änderung an der WebLogic-SSL-Konfiguration für Ihre Domäne vor.
Ändern Sie die Einstellung **Hostname Verification** in `None`.

Beziehen eines Zertifikats von IBM EMM Hosted Services

Zum Konfigurieren der SSL-Kommunikation müssen Sie ein digitales Zertifikat von IBM EMM Hosted Services herunterladen. Die Zertifikatdetails werden in einer Datei mit der Erweiterung `.cer` gespeichert, die Sie in den Keystore des Webanwendungsservers importieren können.

Informationen zu diesem Vorgang

Wenn Ihr bestehendes SSL-Zertifikat abläuft, haben Sie keinen Zugriff mehr auf IBM EMM Hosted Services. Verwenden Sie diese Prozedur, um ein neues Zertifikat herunterzuladen.

Vorgehensweise

1. Melden Sie sich im Internet Explorer bei der Adresse für IBM EMM Hosted Services an, die für Ihr gehostetes E-Mail-Konto konfiguriert wurde.

- Für das Rechenzentrum in den USA lautet die Adresse `https://em.unicaondemand.com`
- Für das Rechenzentrum in Großbritannien lautet die Adresse `https://em-eu.unicaondemand.com`

Der Anmeldeversuch schlägt fehl, ermöglicht Ihnen aber die Übermittlung der Zertifikatsanforderung über den Browser.

2. Klicken Sie auf das Schloss-Symbol und wählen Sie **Zertifikat anzeigen**.
3. Klicken Sie auf die Registerkarte Details und wählen Sie **In Datei kopieren**.

   Speichern Sie die Datei mit einer `.cer`-Erweiterung an einer Speicherposition, auf die der Webanwendungsserver zugreifen kann. Die von Ihnen erstellte Datei ist das digitale Zertifikat, das Sie in den Keystore auf dem Webanwendungsserver einfügen.

   Speichern Sie das Zertifikat beispielsweise unter dem Namen `IBMHosted.cer`.

Erstellen eines vertrauenswürdigen Keystores für WebLogic und Importieren des IBM Zertifikats

Für WebLogic muss ein vertrauenswürdiger Keystore erstellt werden, der das IBM Zertifikat akzeptiert.

Vorbereitende Schritte

Laden Sie zunächst das digitale Zertifikat von IBM EMM Hosted Services über einen Web-Browser herunter, und speichern Sie es als Datei mit der Erweiterung `.cer`. Das Zertifikat kann beispielsweise den Dateinamen `IBMHosted.cer` haben (Sie können auch einen anderen Dateinamen verwenden). Weitere Einzelheiten hierzu finden Sie unter „Beziehen eines Zertifikats von IBM EMM Hosted Services" auf Seite 29.

Informationen zu diesem Vorgang

IBM verwendet die folgenden Stichprobenwerte für die in diesem Abschnitt enthaltenen Prozeduren.

- Identity-Keystore: `IBMUnicaClientIdentity.jks`
- Kennwort für den Identity-Keystore: `clientPwd`
- Vertrauenswürdiger Keystore: `IBMUnicaTrust.jks`
- Alias für den vertrauenswürdigen Keystore: `IBMUnicaHostedIdentity`
- Kennwort (`-storepass`) für den vertrauenswürdigen Keystore: `trustPwd`
- Digitales Zertifikat (`-file`) von IBM: `IBMHosted.cer`

Die tatsächlich einzugebenden Werte müssen sich auf Ihre Installation beziehen.

Um die Schritte dieser Prozedur abzuschließen, führen Sie das Java-Dienstprogramm `keytool` aus der Befehlszeile aus.

Vorgehensweise

1. Generieren Sie einen vertrauenswürdigen Keystore für WebLogic. Ausführliche Informationen hierzu finden Sie im Abschnitt „Generieren eines vertrauenswürdigen Keystores" auf Seite 27.

   Sie geben den *Identity-Keystore* und den *vertrauenswürdigen Keystore* in der WebLogic-Konfiguration an.
2. Verwenden Sie den Befehl `import` im Dienstprogramm `keytool`, um das IBM EMM Hosted Services-Zertifikat zu dem in Schritt 1 erstellten vertrauenswürdi-

gen Keystore hinzuzufügen, wie im folgenden Beispiel dargestellt. Verwenden Sie das von IBM heruntergeladene digitale Zertifikat.

Bei dieser Prozedur definieren Sie auch das Alias für den vertrauenswürdigen Keystore. `keytool -import -alias IBMUnicaHostedIdentity -file <IBMHosted.cer> -keystore <IBMUnicaTrust.jks> -storepass <trustPwd>`

Geben Sie **Y** ein, wenn Sie aufgefordert werden, die Vertrauenswürdigkeit des Zertifikats zu bestätigen.

3. Konfigurieren Sie in der Administrationskonsole von WebLogic die Keystores für den Server.

   Wählen Sie zum Definieren der Konfigurationsregeln die Option für die Keystores 'Custom Identity' (Benutzerdefinierte Identität) und 'Custom Trust' (Benutzerdefinierte Vertrauensstellung) aus den verfügbaren Auswahlmöglichkeiten aus. Geben Sie als 'Custom Identity' den Identity-Keystore an. Geben Sie als 'Custom Trust' den vertrauenswürdigen Keystore an.

   Geben Sie beispielsweise in der Administrationskonsole Folgendes an (wobei Sie die Stichprobenwerte für den in Schritt 1 erstellten vertrauenswürdigen Keystore verwenden).

   - Für **Identity**: Geben Sie den Identity-Keystore und das zugehörige Kennwort an.

     Beispielsweise `IBMUnicaClientIdentity.jks` und `clientPwd`.

   - Für **Trust**: Geben Sie den vertrauenswürdigen Keystore und das zugehörige Kennwort an.

     Beispielsweise `IBMUnicaTrust.jks` und `trustPwd`.

   Geben Sie den vollständigen Pfad zu beiden Keystores an.

4. Starten Sie WebLogic erneut. WebLogic implementiert die Konfigurationsänderungen erst nach einem Neustart des Webanwendungsservers.
5. Um die SSL-Verbindung zu testen, melden Sie sich bei IBM Campaign an und rufen Sie die verschiedenen Menüs mit den Messaging-Funktionen auf. Vergewissern Sie sich, dass Sie E-Mail-Nachrichten, Landing-Pages und Mailings erstellen können.

Konfigurieren von SSL bei Verwendung von IBM WebSphere

Dieser Abschnitt beschreibt die erforderlichen allgemeinen Schritte zum Konfigurieren von SSL, wenn Sie IBM EMM-Komponenten auf IBM WebSphere implementiert haben. Diese Änderung ist erforderlich, damit eMessage-Komponenten, die in Campaign betrieben werden, über SSL mit IBM EMM Hosted Services kommunizieren können.

Vorbereitende Schritte

Bevor Sie beginnen, müssen Sie den Wert für die Konfigurationseigenschaft `uiHostName` kennen. Der Wert für `uiHostName` ist die URL für IBM EMM Hosted Services. Ausführliche Informationen hierzu finden Sie im Abschnitt „Konfigurieren der Adressen zur Verbindungsherstellung mit IBM EMM Hosted Services” auf Seite 25.

Informationen zu diesem Vorgang

Sie müssen auf die WebSphere-Sicherheitskonsole zugreifen, um die Einstellungen für SSL-Zertifikat und Schlüsselmanagement zu ändern. Diese Aufgabe erfordert einen Neustart des Campaign-Webanwendungsservers, damit die Änderungen übernommen werden.

Wenn Sie Campaign auf WebSphere Version 6.1 oder höher implementiert haben, müssen Sie die WebSphere-Sicherheitskonfiguration ändern, um das Unterzeichnerzertifikat von IBM EMM Hosted Services zu beziehen und es zum WebSphere-Truststore hinzuzufügen. Wenn eine Fehlernachricht mit dem Hinweis angezeigt wird, dass Ihr aktuelles Unterzeichnerzertifikat abgelaufen ist, löschen Sie das aktuelle Zertifikat und fügen Sie ein neues hinzu.

Eine genaue Anleitung dazu, wie Sie in der WebSphere-Benutzerschnittstelle navigieren und mit dieser arbeiten, finden Sie in der Dokumentation zu der von Ihnen verwendeten Version von IBM WebSphere.

Anmerkung: Bevor Sie beginnen, vergewissern Sie sich, dass Fixpack 7.0.0.17 auf dem WebSphere-Server installiert wurde. Weitere Informationen finden Sie im Abschnitt „IBM WebSphere Application Server V7.0 erfordert Fixpack 7.0.0.17 oder höher" auf Seite 33.

Vorgehensweise

1. Generieren eines vertrauenswürdigen Keystores.

   Weitere Einzelheiten hierzu finden Sie unter „Generieren eines vertrauenswürdigen Keystores" auf Seite 27.

   Für die Konfiguration von SSL müssen Sie die Werte angeben, die Sie für die folgenden Variablen definieren. Die hier gezeigten Werte sind nur Stichprobenwerte. Ihre Werte können anders lauten.

   - `alias`: *`UnicaClientIdentity`* (Beispiel)
   - `keystore`: *`IBMUnicaTrust.jks`* (Beispiel)
   - `storepass`: *`trustPwd`* (Beispiel)

2. Wählen Sie den neuen Keystore in der WebSphere-Sicherheitskonsole aus.

   Sollten Sie dem Beispiel in Schritt 1 gefolgt sein, dann wählen Sie `IBMUnicaTrust.jks` aus.

3. Beziehen Sie ein Sicherheitszertifikat von IBM EMM Hosted Services und importieren Sie es in WebSphere, wie in den folgenden Schritten beschrieben.

   a. Navigieren Sie in der WebSphere-Sicherheitskonsole zu **SSL-Zertifikat und Schlüsselmanagement** > **Keystores und Zertifikate** > **NodeDefaultTrustStore** > **Unterzeichnerzertifikate**. Wählen Sie die Option **Abrufen von Port** aus.

   b. Konfigurieren Sie WebSphere dafür, eine Testverbindung aufzubauen, um das Unterzeichnerzertifikat von IBM EMM Hosted Services abzurufen. Geben Sie die folgenden Werte für das IBM EMM Hosted Services-Unterzeichnerzertifikat ein.

      - **Host** Der definierte Wert für `eMessage >serverComponentsAndLocations > hostedServices >uiHostName`
      - **Port** 443
      - **SSL-Konfiguration für abgehende Verbindungen** `NodeDefaultSSLSettings`
      - **Alias** Der Wert, den Sie für **Host** eingegeben haben

      Wenn Sie dies abgeschlossen haben, kommuniziert WebSphere mit IBM EMM Hosted Services, um die erforderlichen Informationen zum Erstellen eines Unterzeichnerzertifikats für IBM EMM Hosted Services abzurufen.

4. Nachdem WebSphere die Erstellung des Unterzeichnerzertifikats abgeschlossen hat, wählen Sie das neue Zertifikat in der Sicherheitskonsole aus.

Der Webanwendungsserver verwendet das neue Zertifikat beim Aufbauen von Verbindungen zu IBM EMM Hosted Services.

5. Starten Sie WebSphere erneut.

   WebSphere implementiert die Konfigurationsänderungen erst, nachdem Sie den Webanwendungsserver erneut gestartet haben.

IBM WebSphere Application Server V7.0 erfordert Fixpack 7.0.0.17 oder höher

Falls Sie vorhaben, IBM WebSphere Application Server V7.0 für die Implementierung von IBM EMM-Produkten zu verwenden, müssen Sie das Fixpack 17 (auch als Version 7.0.0.17 bekannt) oder höher ausführen, um ein Sicherheitsproblem zu beseitigen. Dies gilt für sämtliche Pakete von WebSphere Application Server 7.0, auch für die Version, die im Produktpaket mancher IBM EMM-Produkte enthalten ist.

Sie können das Fixpack 17 oder höher hier beziehen:

http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg27013594.

Beachten Sie, dass Sie auf dieser Seite vor dem Herunterladen das korrekte Fixpack auswählen müssen.

Weitere Informationen zu unterstützten WebSphere-Versionen für die Implementierung von IBM EMM-Produkten finden Sie im Dokument *Empfohlene Softwareumgebungen und Mindestsystemvoraussetzungen* zu jedem Produkt.

Kapitel 4. RCT (Response and Contact Tracker)

Der Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) wird in Ihrer lokalen Umgebung installiert und kommuniziert mit IBM EMM Hosted Services, um Daten für E-Mail-Kontakte, E-Mail-Zustellung und Empfängerantworten, wie z. B. Link-Klicks, abzurufen und zu verarbeiten. Der RCT muss aktiv sein, um Daten zur Linkverfolgung und E-Mail-Zustellungsbenachrichtigung von IBM EMM Hosted Services abrufen zu können.

Der Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) wird in Ihrer lokalen Umgebung installiert und kommuniziert mit IBM EMM Hosted Services, um Daten für E-Mail-Kontakte, E-Mail-Zustellung und Empfängerantworten, wie z. B. Link-Klicks, abzurufen und zu verarbeiten. Der RCT muss aktiv sein, um Daten zur Linkverfolgung und E-Mail-Zustellungsbenachrichtigung von IBM EMM Hosted Services abrufen zu können.

Sie können den RCT auf eine der folgenden Arten starten.

- Starten Sie den RCT manuell.
- Starten Sie den RCT als Service.

Wichtig: Sie müssen den RCT bei der ersten Verwendung von eMessage manuell starten, selbst wenn Sie den RCT als Service registriert haben.

Sie müssen den RCT erneut starten, wenn Sie Änderungen an Konfigurationseigenschaften für eMessage vornehmen. Sie können den RCT jederzeit erneut starten, selbst wenn Sie ihn für die Ausführung als Service konfiguriert haben. IBM EMM Hosted Services setzt die Speicherung von Verfolgungsdaten fort, wenn der RCT beendet oder erneut gestartet wird. Wenn der RCT den Betrieb wieder aufnimmt, lädt er die in die Warteschlange gestellten Informationen herunter.

Zugehörige Konzepte:

„Downloadrate für Daten und Porteinstellung" auf Seite 23

„RCT manuell starten"

„Informationen zum automatischen Starten des RCT als Service" auf Seite 36

RCT manuell starten

Der RCT (Response and Contact Tracker) wird mit dem Script `rct` gestartet bzw. gestoppt. Soll der RCT manuell gestartet werden, führen Sie das Script `rct` im Verzeichnis `bin` Ihrer eMessage-Installation aus.

Weitere Informationen zu diesem Script finden Sie unter „eMessage-Script für den Response and Contact Tracker (RCT)" auf Seite 98.

Zugehörige Konzepte:

Kapitel 4, „RCT (Response and Contact Tracker)"

© Copyright IBM Corp. 1999, 2015

Manueller Betrieb des RCT (Response and Contact Tracker)

Soll der RCT (Response and Contact Tracker) manuell betrieben werden, müssen Sie im Verzeichnis `bin` Ihrer eMessage-Installation das Script `rct` ausführen.

Vorgehensweise

- Um den RTC zu starten, führen Sie wie folgt im Verzeichnis `bin` Ihrer eMessage-Installation das Script `rct` aus.

  ```
  rct start
  ```

- Um den RCT zu stoppen, führen Sie wie folgt das Script `rct` aus.

  ```
  rct stop
  ```

Nächste Schritte

Weitere Informationen zu diesem Script finden Sie unter „eMessage-Script für den Response and Contact Tracker (RCT)" auf Seite 98.

Response and Contact Tracker stoppen

Stoppen Sie den Response and Contact Tracker, indem Sie das Script `rct` ausführen.

Vorgehensweise

Führen Sie im Verzeichnis `bin` Ihrer eMessage-Installation das Script `rct` wie folgt aus.

```
rct stop
```

Nächste Schritte

IBM EMM Hosted Services speichert weiterhin empfangene Verfolgungs- und Antwortdaten, bis Sie den RCT erneut starten.

Weitere Informationen zu diesem Script finden Sie im Abschnitt „eMessage-Script für den Response and Contact Tracker (RCT)" auf Seite 98.

Informationen zum automatischen Starten des RCT als Service

Sie können den Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) auf automatischen Start konfigurieren, indem Sie ihn als Service hinzufügen.

Sie können den RCT-Service registrieren, indem Sie das mit der eMessage-Software bereitgestellte Script `MKService_rct` ausführen.

Wenn Sie das Script `MKService_rct` zum Registrieren des Dienstes ausführen, müssen Sie das Script `rct` verwenden, um den RCT-Service erstmalig manuell zu starten. Danach wird der RCT jedes Mal automatisch gestartet, wenn Sie das Betriebssystem der Maschine, auf der der RCT installiert ist, erneut starten.

Nachdem Sie den RCT-Service konfiguriert haben, können Sie den automatischen Start der RCT verhindern, indem Sie das Script `MKService_rct` mit der Option `-remove` ausführen.

Zugehörige Konzepte:

Kapitel 4, „RCT (Response and Contact Tracker)", auf Seite 35

Zugehörige Tasks:

„Response and Contact Tracker als Service hinzufügen”

„RCT-Service entfernen” auf Seite 38

Zugehörige Verweise:

„eMessage-Script 'MKService_rct'” auf Seite 99

Response and Contact Tracker als Service hinzufügen

Sie können den Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) auf automatischen Start konfigurieren, indem Sie ihn als Service hinzufügen.

Informationen zu diesem Vorgang

Sie können den RCT-Service registrieren, indem Sie das mit der eMessage-Software bereitgestellte Script `MKService_rct` ausführen.

Soll der RCT (Response and Contact Tracker) als Service hinzugefügt werden, führen Sie im Verzeichnis `bin` Ihrer eMessage-Installation das Script `MKService_rct -install` aus.

Das Verzeichnis `bin` wird bei der Installation von IBM Campaign bzw. bei einem Upgrade auf die aktuellste Version als Unterverzeichnis im Installationsverzeichnis von Campaign erstellt.

Vorgehensweise

Soll der RCT (Response and Contact Tracker) als Service hinzugefügt werden, führen Sie im Verzeichnis `bin` Ihrer eMessage-Installation das Script `MKService_rct -install` aus.
Führen Sie in UNIX oder Linux-Umgebungen dieses Script mit einem Benutzer aus, der über Rootberechtigungen verfügt oder berechtigt ist, Dämonprozesse zu erstellen.
In Windows lautet der Name des Dienstes **Response & Contact Tracker**.

Nächste Schritte

Starten Sie nach der Ausführung des Scripts `MKService_rct` den RCT manuell mit dem Script `rct`. Sie müssen den RCT nur einmal neu starten. Nachdem Sie den RCT erstmalig manuell gestartet haben, wird er jedes Mal automatisch gestartet, wenn Sie das Betriebssystem des Computers, auf dem Sie den RCT installiert haben, erneut starten.

Nachdem Sie den RCT-Service konfiguriert haben, können Sie den automatischen Start der RCT verhindern, indem Sie das Script `MKService_rct` mit der Option `-remove` ausführen.

Zugehörige Konzepte:

„Informationen zum automatischen Starten des RCT als Service” auf Seite 36

Zugehörige Verweise:

„eMessage-Script 'MKService_rct'” auf Seite 99

„eMessage-Script für den Response and Contact Tracker (RCT)” auf Seite 98

RCT-Service entfernen

Wenn der RCT (Response and Contact Tracker) als Service installiert wurde, wird er bei jedem Neustart des Systems, auf dem er installiert ist, ebenfalls gestartet. Um den automatischen Neustart des RCT zu verhindern, müssen Sie den RCT-Service entfernen.

Vorgehensweise

Um den RCT als Service zu entfernen, führen Sie das Script `MKService_rct` unter Angabe der Option `-remove` aus.
Führen Sie aus einer Windows-Befehlszeile in Ihrem IBM EMM-Ausgangsverzeichnis den Befehl `eMessage\bin\MKService_rct.bat -remove` aus.
Führen Sie in UNIX oder Linux in Ihrem IBM EMM-Ausgangsverzeichnis den Befehl `eMessage/bin/MKService_rct.sh -remove` aus.

Nächste Schritte

Weitere Informationen zu diesem Script finden Sie im Abschnitt „eMessage-Script 'MKService_rct'" auf Seite 99.

Zugehörige Konzepte:

„Informationen zum automatischen Starten des RCT als Service" auf Seite 36

Kapitel 5. Überprüfung beim Start

Um sicherzustellen, dass Sie Zugriff auf alle Funktionen für gehostete E-Mail haben, sollten Sie die Konfigurationen und Verbindungen für Ihre Campaign- und eMessage-Installationen nach der Aktivierung von eMessage, nach einer Erweiterung der eMessage-Installation oder nach einem Upgrade der Campaign-Installation testen.

Überprüfen Sie die Konfigurationen und Verbindungen nach der Ausführung einer der folgenden Aktionen:

- Erstmaliges Aktivieren von eMessage
- Aktualisieren Ihrer aktuellen IBM Campaign-Installation
- Hinzufügen einer neuen Partition zu der in IBM Marketing Platform gespeicherten eMessage-Konfiguration

Prüfung der Systemkonfigurationen

Um sicherzustellen, dass die Startvorbereitungen abgeschlossen sind, vergewissern Sie sich, dass die folgenden Konfigurationseigenschaften festgelegt wurden und dass die Einstellungen die Anforderungen für Ihre eMessage- und Campaign-Installationen erfüllen.

Konfigurationseigenschaft	Einstellung
`Campaign | partitions | partition[n] | eMessage | eMessagePluginJarFile`	Vollständiger Pfad zur Speicherposition der Plug-in-Datei, die als Recipient List Uploader (RLU) agiert. Geben Sie das vollständige lokale Verzeichnis im Dateisystem des Computers ein, der den Campaign-Webanwendungsserver hostet. Das IBM Installationsprogramm trägt bei Ihrer Ausführung der Installation diese Einstellung automatisch für die Standardpartition ein. Für andere Partitionen müssen Sie diese Eigenschaft manuell konfigurieren.
`Campaign | partitions | partition[n] | server | internal | eMessageInstalled`	Gibt an, dass eMessage installiert ist. Setzen Sie diese Eigenschaft in jeder Partition, in der Sie eMessage aktivieren möchten, auf **Yes** (Ja). Dies gilt auch für die Standardpartition. Wenn Sie diese Eigenschaft auf **Yes** setzen, sind die eMessage-Funktionen in der Campaign-Schnittstelle verfügbar.
`eMessage | serverComponentsAndLocations | hostedServices | uiHostName`	Adresse von IBM EMM Hosted Services für die gesamte Kommunikation (mit Ausnahme des Uploads von Listen). Die Standardeinstellung lautet bei dem Rechenzentrum in den USA `em.unicaondemand.com`. Wenn Sie sich mit dem Rechenzentrum in Großbritannien verbinden, ändern Sie diesen Wert in `em-eu.unicaondemand.com`.
`eMessage | serverComponentsAndLocations | hostedServices | dataHostName`	Die Adresse für die Verbindung, die von eMessage für den Upload von Metadaten an IBM EMM Hosted Services verwendet wird, die mit den Empfängerlisten zusammenhängen. Die Standardeinstellung lautet bei dem Rechenzentrum in den USA `em.unicaondemand.com`. Wenn Sie sich mit dem Rechenzentrum in Großbritannien verbinden, ändern Sie diesen Wert in `em-eu.unicaondemand.com`.

© Copyright IBM Corp. 1999, 2015

Konfigurationseigenschaft	Einstellung
eMessage | serverComponentsAndLocations | hostedServices | ftpHostName	Die Adresse für die Verbindung, über die eMessage Empfängerlistendaten (ausgenommen Listenmetadaten) an IBM EMM Hosted Services hochlädt. Die Standardeinstellung lautet bei dem Rechenzentrum in den USA ftp-em.unicaondemand.com. Wenn Sie sich mit dem Rechenzentrum in Großbritannien verbinden, ändern Sie diesen Wert in ftp-em-eu.unicaondemand.com.
eMessage | partitions | partition[n] | hostedAccountInfo | amUserForAcctCredentials	Der IBM EMM-Benutzer, der die Datenquelle referenziert, die die Zugriffsberechtigungsnachweise für IBM EMM Hosted Services enthält. Sie konfigurieren diesen Wert, wenn Sie einen Systembenutzer für den Zugriff auf die E-Mail-Ressourcen erstellen, die von IBM gehostet werden.
eMessage | partitions | partition[n] | hostedAccountInfo | amDataSourceForAcctCredentials	Die Marketing Platform-Datenquelle, die die Anmeldeberechtigungsnachweise für IBM EMM Hosted Services enthält. Sie konfigurieren diesen Wert, wenn Sie einen Systembenutzer für den Zugriff auf die E-Mail-Ressourcen erstellen, die von IBM gehostet werden.
eMessage | partitions | partition [n] < dataSources | systemTables | type	Der Typ der Datenbank, die die Systemtabellen enthält. Geben Sie den entsprechenden Wert für Ihre Datenbank an.
eMessage | partitions | partition [n] < dataSources | systemTables | schemaName	Der Name des Datenbankschemas für die Systemtabellen. Geben Sie den entsprechenden Schemanamen für Ihre Datenbank an.
eMessage | partitions | partition [n] < dataSources | systemTables | jdbcClassName	Der JDBC-Treiber für Systemtabellen. Geben Sie den entsprechenden Wert für Ihre Umgebung an.
eMessage | partitions | partition [n] < dataSources | systemTables | jdbcURI	Der URI der JDBC-Verbindung für Systemtabellen. Geben Sie den entsprechenden Wert für Ihre Umgebung an. Geben Sie den Datenbanktyp, den Datenbanktreiber, den Host, den Port und den Datenbanknamen an. Beispiel: jdbc:oracle:thin:@yourdb.example.com:1234:DBname In der Dokumentation Ihrer Datenbank finden Sie genaue Anweisungen für das Erstellen der JDBC-URL. Der von Ihnen eingegebene Wert muss exakt mit dem Wert übereinstimmen, der in Ihrem Campaign-Web-Server definiert ist.
eMessage | partitions | partition [n] < dataSources | systemTables | asmUserForDBCredentials	Der IBM EMM-Benutzer, der die Datenquelle referenziert, die die Anmeldeberechtigungsnachweise für Systemtabellen enthält. Sie erstellen diesen Benutzer, wenn Sie den Zugriff auf die lokalen eMessage-Systemtabellen konfigurieren.
eMessage | partitions | partition [n] < dataSources | systemTables | asmDataSourceForDBCredentials	Die Marketing Platform-Datenquelle, die die Anmeldeberechtigungsnachweise für die Datenbank mit den Systemtabellen enthält. Sie erstellen diese Datenquelle, wenn Sie einen Benutzer für den Zugriff auf die eMessage-Systemtabellen erstellen.

Zugehörige Konzepte:

Kapitel 6, „Konfigurationen für IBM eMessage", auf Seite 43

Zugehörige Tasks:

„Systembenutzer mit Zugriff auf IBM EMM Hosted Services konfigurieren" auf Seite 24

„Konfiguration des Zugriffs auf lokale eMessage-Systemtabellen" auf Seite 48

Upload an IBM EMM Hosted Services testen

Um die Fähigkeit zum Hochladen von Daten aus Ihrer lokalen Umgebung an IBM EMM Hosted Services zu testen, müssen Sie das Script **rlu** im Prüfmodus ausführen.

Vorgehensweise

Führen Sie im Verzeichnis `bin` Ihrer eMessage-Installation das Script `rlu` auf eine der folgenden Arten aus.

- `rlu -c`
- `rlu --check`

Zugehörige Verweise:

„RLU-Script" auf Seite 97

Download aus IBM EMM Hosted Services testen

Um die Fähigkeit zum Herunterladen von Informationen aus IBM EMM Hosted Services zu testen, müssen Sie das Script **rct** im Prüfmodus ausführen.

Vorgehensweise

Führen Sie im Verzeichnis `bin` Ihrer eMessage-Installation das Script `rct` wie folgt aus.

```
rct check
```

Zugehörige Verweise:

„eMessage-Script für den Response and Contact Tracker (RCT)" auf Seite 98

Verbindung mit der gehosteten Messaging-Schnittstelle testen

IBM betreibt die Messaging-Schnittstelle über die IBM Rechenzentren in den USA und in Großbritannien. Testen Sie die Verbindung zur gehosteten Mailing-Schnittstelle, indem Sie versuchen, eine eMessage-Funktion aufzurufen.

Vorgehensweise

Melden Sie sich bei IBM EMM an und wählen Sie im **Campaign**-Menü die Option **eMessage mailings** (eMessage-Mailings) aus.
Wenn die Verbindung mit der eMessage-Benutzerschnittstelle ordnungsgemäß aufgebaut wird, wird die Seite der eMessage-Mailings geöffnet. Dort wird eine Liste mit den Mailings und zugehörigen Mailing-Merkmalen angezeigt.
Falls die Verbindung mit der Benutzerschnittstelle nicht ordnungsgemäß aufgebaut werden kann, wird ein Fehler angezeigt.

Kapitel 6. Konfigurationen für IBM eMessage

Die IBMMarketing Platform stellt mehrere Konfigurationseigenschaften zur Verfügung, mit denen das Verhalten und das Aussehen von IBMeMessage geändert werden können. Manche Konfigurationseigenschaften werden während der Installation festgelegt. Sie können Konfigurationseigenschaften jederzeit ändern.

Nachdem Sie Campaign- oder eMessage-Konfigurationen aktualisiert haben, müssen Sie den Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) und den Webanwendungsserver, auf dem sich Campaign befindet, erneut starten.

Merkmal oder Funktion	**Konfigurationseigenschaft (einschließlich Pfad)**
Aktivieren oder Inaktivieren von eMessage in der Campaign-Partition. Siehe „Campaign | Partitionen | Partition[n] | Server | intern" auf Seite 50.	`Campaign | partitions | partition[n] | server | internal`
Merkmale von E-Mail-Empfängerlisten. Siehe „Campaign | Partitionen | Partition[n] | eMessage" auf Seite 49.	`Campaign | partitions | partition[n] | eMessage`
Erforderliche URLs zum Herstellen der Verbindung zu IBM EMM Hosted Services. Siehe „eMessage | serverComponentsAndLocations | hostedServices" auf Seite 55.	`eMessage | serverComponentsAndLocations | hostedServices`
Datenbank- und Kontozugriffsberechtigungen zum Herstellen der Verbindung zu IBM EMM Hosted Services. Siehe „eMessage | Partitionen | Partition[n] | hostedAccountInfo" auf Seite 56.	`eMessage | partitions | partition[n] | hostedAccountInfo`
Datenbankzugriff und Schemaeinstellungen für die eMessage-Systemtabellen. Siehe „eMessage | Partitionen | Partition[n] | dataSources | systemTables" auf Seite 57.	`eMessage | partitions | partition[n] | dataSources | systemTables`
Speicherposition eines Scripts, das als Antwort auf die Aktionen oder den Status des Hochladeprogramms für die Empfängerliste (RLU) ausgeführt wird (optional). Siehe „eMessage | Partitionen | Partition[n] | recipientListUploader" auf Seite 60.	`eMessage | partitions | partition[n] | recipientListUploader`

© Copyright IBM Corp. 1999, 2015

Merkmal oder Funktion	Konfigurationseigenschaft (einschließlich Pfad)
Einstellungen im Zusammenhang mit dem Datendownload, die vom Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) verarbeitet werden. Siehe „eMessage | partitions | partition[n] | responseContactTracker" auf Seite 60.	`eMessage | partitions | partition[n] | responseContactTracker`
Unterstützung für die Anzeige von Listen mit personalisierten Daten in eMessage auf Basis von Dimensionstabellen in Campaign. Siehe . Konfigurieren der Unterstützung für Dimensionstabellen.	`Campaign | partitions | partition[n]| eMessage | oltDimTableSupport`
Unterstützung der Verfolgung des Mailing-Ausführungsprotokolls. Siehe „eMessage | partitions | partition[n] | responseContactTracker" auf Seite 60.	`eMessage | partitions | partition[n] | responseContactTracker` Weitere Informationen finden Sie in der Beschreibung des Parameters **`enableExecutionHistoryDataTracking`**.

Weitere Informationen zum Arbeiten mit Konfigurationseigenschaften finden Sie im *IBM Marketing Platform-Administratorhandbuch*.

Zugehörige Konzepte:

„Prüfung der Systemkonfigurationen" auf Seite 39

Für eMessage zu konfigurierende Aspekte

Sie können die folgenden Aspekte der lokalen Installation von IBM eMessage konfigurieren.

Merkmal oder Funktion	Konfigurationseigenschaft (einschließlich Pfad)
Aktivieren oder Inaktivieren von eMessage in der Campaign-Partition. Siehe „Campaign | Partitionen | Partition[n] | Server | intern" auf Seite 50.	`Campaign | partitions | partition[n] | server | internal`
Merkmale von E-Mail-Empfängerlisten. Siehe „Campaign | Partitionen | Partition[n] | eMessage" auf Seite 49.	`Campaign | partitions | partition[n] | eMessage`
Erforderliche URLs zum Herstellen der Verbindung zu IBM EMM Hosted Services. Siehe „eMessage | serverComponentsAndLocations | hostedServices" auf Seite 55.	`eMessage | serverComponentsAndLocations | hostedServices`
Datenbank- und Kontozugriffsberechtigungen zum Herstellen der Verbindung zu IBM EMM Hosted Services. Informationen hierzu finden Sie in „eMessage | Partitionen | Partition[n] | hostedAccountInfo" auf Seite 56.	`eMessage | partitions | partition[n] | hostedAccountInfo`

Merkmal oder Funktion	Konfigurationseigenschaft (einschließlich Pfad)
Datenbankzugriff und Schemaeinstellungen für die eMessage-Systemtabellen. Informationen hierzu finden Sie in „eMessage | Partitionen | Partition[n] | dataSources | systemTables" auf Seite 57.	`eMessage | partitions | partition[n] | dataSources | systemTables`
Speicherposition eines Scripts, das als Antwort auf die Aktionen oder den Status des Hochladeprogramms für die Empfängerliste (RLU) ausgeführt wird (optional). Informationen hierzu finden Sie in „eMessage | Partitionen | Partition[n] | recipientListUploader" auf Seite 60.	`eMessage | partitions | partition[n] | recipientListUploader`
Einstellungen im Zusammenhang mit dem Datendownload, die vom Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) verarbeitet werden. Informationen hierzu finden Sie in „eMessage | partitions | partition[n] | responseContactTracker" auf Seite 60.	`eMessage | partitions | partition[n] | responseContactTracker`
Unterstützung für die Anzeige von Listen mit personalisierten Daten in eMessage auf Basis von Dimensionstabellen in Campaign. Siehe „Konfigurieren der Unterstützung für Dimensionstabellen" auf Seite 47.	`Campaign | partitions | partition[n] | eMessage | oltDimTableSupport`
Unterstützung der Integration von Campaign-Angeboten in personalisierte E-Mails. Informationen hierzu finden Sie in „Campaign | Partitionen | Partition[n] | eMessage | contactAndResponseHistTracking" auf Seite 53.	`Campaign | partitions | partition[n] | eMessage | contactAndResponseHistTracking`
Unterstützung der Verfolgung des Mailing-Ausführungsprotokolls. Informationen hierzu finden Sie in „eMessage | partitions | partition[n] | responseContactTracker" auf Seite 60.	`eMessage | partitions | partition[n] | responseContactTracker` Weitere Informationen finden Sie in der Beschreibung des Parameters **`enableExecutionHistoryDataTracking`**.

Nach Konfigurationsänderungen erneut zu startende Komponenten

Nach Änderungen an den Campaign- oder eMessage-Konfigurationen müssen Sie den Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) und den Webanwendungsserver, auf dem sich Campaign befindet, erneut starten.

Informationen zum Neustart des RCT finden Sie im Abschnitt „eMessage-Script für den Response and Contact Tracker (RCT)" auf Seite 98.

Informationen zum erneuten Starten des Webanwendungsservers sind in der Dokumentation zu Ihrem Webanwendungsserver enthalten.

Zugriff auf zusätzliches Protokoll der Mailing-Ausführung konfigurieren

Sie können anfordern, dass IBM zusätzliche Daten für das Protokoll der Mailing-Ausführung bereitstellt. Der Zugriff auf zusätzliche Daten für das Protokoll der Mailing-Ausführung kann bei IBM angefordert werden. Hierfür müssen Sie auch die eMessage-Konfiguration aktualisieren. Die Daten für das Protokoll der Mailing-Ausführung werden in Ihren lokalen eMessage-Systemtabellen in der Tabelle `UACE_ExecHistory` aufgezeichnet. Sie beschreiben abgeschlossene Mailing-Ausführungen.

Vorbereitende Schritte

Zum Download zusätzlicher Daten der Mailing-Ausführung müssen Sie die Konfigurationseigenschaft `enableExecutionHistoryDataTracking` aktualisieren. `enableExecutionHistoryDataTracking` ist standardmäßig nicht in den Konfigurationseigenschaften von eMessage verfügbar.

Sie können diese Konfigurationseigenschaft in Ihrer lokalen eMessage-Installation anzeigen, indem Sie das Script `switch_config_visibility.bat` ausführen, das sich im Verzeichnis `emessage\tools` befindet.

Informationen zu diesem Vorgang

Die folgenden Arten von Datensätzen sind verfügbar, wenn Sie Campaign Version 8.6.0.4 oder Version 9.1.0 und neuere Versionen installieren. Bei der Version 9.0.0 sind diese Informationen nicht verfügbar.

- Betreffzeile der Nachricht
- Adresse des Absenders
- Benutzer, der das Mailing aktualisiert hat
- Dokumentbeschreibung
- Speicherdatum des Mailings

Vorgehensweise

1. Fordern Sie den Zugriff auf zusätzliche Protokolldaten der Mailing-Ausführung an. Um den Zugriff anzufordern, wenden Sie sich an Ihren IBM Ansprechpartner unter `eacctsvc@us.ibm.com`.
2. Aktualisieren Sie die eMessage-Konfiguration. Konfigurieren Sie die folgende Konfigurationseigenschaft.

`Affinium|eMessage|partitions|partition1|responseContactTracker|`
`enableExecutionHistoryDataTracking`

Setzen Sie **`enableExecutionHistoryDataTracking`** auf **True**.

Nächste Schritte

Sie können die eMessage-Systemtabellen abfragen, um Informationen zur Mailing-Ausführung aus der Tabelle `UACE_ExecHistory` abzurufen.

Weitere Informationen zu den eMessage-Systemtabellen finden Sie im Handbuch *IBM EMM System Tables and Data Dictionary*.

Zugehörige Tasks:

„Zugriff auf die Konfigurationsparameter zum Hochladen von Daten mit implizitem FTP" auf Seite 16

Unterstützung für die Integration von Campaign-Angeboten

IBM eMessage unterstützt das Hinzufügen von in Campaign konfigurierten Angeboten zu personalisierter E-Mail, die in eMessage erstellt wurde.

Die Angebote basieren auf Angebotsvorlagen, die in IBM Campaign konfiguriert wurden. Zur Unterstützung der Integration von Campaign-Angeboten in personalisierter E-Mail müssen Sie die Eigenschaft `contactAndResponseHistTracking` in der Campaign-Konfiguration entsprechend anpassen und weitere Campaign-Einstellungen vornehmen.

Weitere Informationen zur Konfiguration der Unterstützung für die Angebotsintegration finden Sie in den Abschnitten zur eMessage-Angebotsintegration im *IBM Campaign-Administratorhandbuch*.

Zugehörige Verweise:

„Campaign | Partitionen | Partition[n] | eMessage | contactAndResponseHistTracking" auf Seite 53

Konfigurieren der Unterstützung für Dimensionstabellen

Damit bestimmte Funktionen unterstützt werden, die von erweiterten Scripts für E-Mails bereitgestellt werden, muss die Konfigurationseigenschaft `oltDimTableSupport` auf **True** gesetzt werden. Bei einem Upgrade auf Campaign 8.5.0 oder höher muss der Wert dieser Konfigurationseigenschaft manuell geändert werden.

Informationen zu diesem Vorgang

eMessage stellt erweiterte Scripts für die Erstellung von E-Mail-Nachrichten bereit, die Listen mit individuellen Kontaktdaten enthalten. Diese Listen erfordern, dass verknüpfte Dimensionstabellen in Campaign erstellt werden, die eine Ausgabelistentabelle (OLT) enthalten, die die E-Mail-Empfängerliste definiert. Ausgabelistentabellen werden im eMessage-Schema erstellt.

Die Konfigurationseigenschaft `oltDimTableSupport` steuert die Unterstützung für die Erstellung von Dimensionstabellen im eMessage-Schema. Wenn der Wert für diese Eigenschaft auf `True` festgelegt ist, kann eine OLT in einer Dimensionstabelle bereitgestellte Informationen verwenden. Vor Campaign 8.5.0 war der Standardwert für `oltDimTableSupport` nicht `True`, sondern `False`.

Gehen Sie wie folgt vor, um die Eigenschaft `oltDimTableSupport` zu aktualisieren.

Weitere Informationen dazu, wie Marketiers erweiterte Scripts zum Erstellen von Datentabellen verwenden, finden Sie im *IBM eMessage-Benutzerhandbuch*.

Vorgehensweise

1. Navigieren Sie zu **Settings** > **Configuration** > **Campaign** > **Partitions** > **partition[n]** > **eMessage** (Einstellungen > Konfiguration > Campaign > Partitionen > Partition[n] > eMessage).
2. Klicken Sie auf **Edit Settings** (Einstellungen bearbeiten) und setzen Sie den Wert der Eigenschaft `oltDimTableSupport` auf `True`.

Konfiguration des Zugriffs auf lokale eMessage-Systemtabellen

Die eMessage-Komponenten müssen in der Lage sein, auf die eMessage-Systemtabellen im Campaign-Schema zuzugreifen. Sie müssen einen Systembenutzer erstellen und konfigurieren, der automatisch auf die Systemtabellen zugreifen kann. Der bei der Installation von Campaign konfigurierte Systembenutzer verfügt bereits über den erforderlichen Zugriff auf das Campaign-Schema.

Informationen zu diesem Vorgang

Anmerkung: Wenn Ihre Installation mehrere Partitionen enthält, müssen Sie diese Aufgabe für jede Partition ausführen. Systembenutzer können nicht partitionsübergreifend gemeinsam genutzt werden.

Wenn ein anderer Systembenutzer auf die eMessage-Systemtabellen zugreifen soll, müssen Sie einen neuen Systembenutzer in der Marketing Platform und eine neue Plattformdatenquelle mit Zugriff auf das Campaign-Schema erstellen.

Vorgehensweise

1. Geben Sie in der eMessage-Konfiguration einen Systembenutzer an, der auf die Datenbank zugreift, die das Campaign-Schema hostet.

   Sie können einen neuen Benutzer erstellen oder einen vorhandenen Benutzer angeben. Der Systembenutzer, den Sie für Campaign eingerichtet haben, verfügt bereits über Zugriff auf das Campaign-Schema.

   Verwenden Sie die Konfigurationseigenschaft `eMessage > partitions > partition [n] < dataSources > systemTables > asmUserForDBCredentials`.

   Standardmäßig ist der Benutzer `asm_admin` angegeben.
2. Geben Sie in der eMessage-Konfiguration die Datenquelle an, die so konfiguriert wurde, dass sie den Benutzernamen und das Kennwort enthält, die für den Zugriff auf die Datenbank mit dem Campaign-Schema benötigt werden.

   Sie können die Datenquelle verwenden, die bei der Installation von Campaign für den Zugriff auf das Campaign-Schema erstellt wurde.

   Verwenden Sie die Konfigurationseigenschaft `eMessage > partitions > partition [n] < dataSources > systemTables > amDataSourceForDBCredentials`.

Zugehörige Konzepte:

„Prüfung der Systemkonfigurationen" auf Seite 39

Konfigurationseigenschaften für eMessage

Die Konfigurationseigenschaften für eMessage erreichen Sie über das Menü "Einstellungen" in der Marketing Platform. Die Eigenschaften zum Konfigurieren von eMessage sind in den Konfigurationskategorien "Campaign" und "eMessage" enthalten.

Um auf die Konfigurationseigenschaften zuzugreifen, navigieren Sie zu **Einstellungen > Konfigurationen**. Auf der Seite "Konfigurationen" werden alle verfügbaren Konfigurationseigenschaften für Ihre IBM EMM-Installation aufgelistet.

Campaign | Partitionen | Partition[n] | eMessage

In dieser Kategorie werden Eigenschaften definiert, um Kenndaten von Empfängerlisten zu definieren und die Position von Ressourcen anzugeben, die die Listen in IBM EMM Hosted Services hochladen.

eMessagePluginJarFile

Beschreibung

Vollständiger Pfad zur Position der Datei, die als Recipient List Uploader (RLU) fungiert. Dieses Plug-in für Campaign lädt OLT-Daten und zugehörige Metadaten in die fernen von IBM gehosteten Services hoch. Bei der angegebenen Position muss es sich um den vollständigen Pfad des lokalen Verzeichnisses im Dateisystem des Computers handeln, der den Campaign-Webanwendungsserver hostet.

Das IBM Installationsprogramm belegt diese Einstellung automatisch für die Standardpartition, wenn das Installationsprogramm ausgeführt wird. Für andere Partitionen muss diese Eigenschaft manuell konfiguriert werden. Da es nur einen RLU für jede eMessage-Installation gibt, müssen alle Partitionen dieselbe Position für den RLU angeben.

Ändern Sie diese Einstellung nur, wenn IBM Sie dazu auffordert.

Standardwert

Es ist kein Standardwert definiert.

Gültige Werte

Vollständiger Pfad des lokalen Verzeichnisses, in dem Sie den Campaign-Web-Server installiert haben.

defaultSeedInterval

Beschreibung

Die Anzahl Nachrichten zwischen Seednachrichten, falls `defaultSeedType` `Distribute list` ist.

Standardwert

`1000`

defaultSeedType

Beschreibung

Die Standardmethode, die eMessage verwendet, um Seedadressen in eine Empfängerliste einzufügen.

Standardwert

`Distribute IDS`

Gültige Werte

- `Distribute IDS` – Damit werden IDs basierend auf der Größe der Empfängerliste und der Anzahl verfügbarer Seedadressen gleichmäßig verteilt und Seedadressen werden in gleichmäßigen Intervallen in die gesamte Empfängerliste eingefügt.
- `Distribute list` – Damit wird die Seedadresse für jede `defaultSeedInterval`-ID in die Hauptliste eingefügt. Es wird die gesamte Liste verfüg-

barer Seedadressen in bestimmten Intervallen in die gesamte Empfängerliste eingefügt. Sie müssen das Intervall zwischen den Einfügepunkten angeben.

oltTableNamePrefix

Beschreibung

Wird im erstellten Schema für die Ausgabelistentabelle verwendet. Sie müssen diesen Parameter definieren.

Standardwert

OLT

Gültige Werte

Das Präfix kann nicht mehr als acht alphanumerische Zeichen oder Unterstreichungszeichen enthalten und muss mit einem Buchstaben beginnen.

oltDimTableSupport

Beschreibung

Dieser Konfigurationsparameter steuert die Möglichkeit, Ausgabelistentabellen (Output List Table, OLT), die im eMessage-Schema erstellt wurden, Dimensionstabellen hinzuzufügen. Dimensionstabellen sind erforderlich, um erweitertes Scripting für E-Mail zu verwenden und damit Datentabellen in E-Mail-Nachrichten zu erstellen.

Die Standardeinstellung ist `False`. Sie müssen diese Eigenschaft auf `True` setzen, damit Marketiers Dimensionstabellen erstellen können, wenn sie den eMessage-Prozess verwenden, um eine Empfängerliste zu definieren. Weitere Informationen zum Erstellen von Datentabellen und zur Arbeit mit erweiterten Scripts für E-Mail finden Sie im *IBM eMessage Benutzerhandbuch*.

Standardwert

False

Gültige Werte

True | False

Campaign | Partitionen | Partition[n] | Server | intern

Die Eigenschaften in dieser Kategorie geben die Integrationseinstellungen und die Grenzwerte der internen IDs für die ausgewählte Campaign-Partition an. Wenn Ihre Campaign-Installation über mehrere Partitionen verfügt, legen Sie diese Eigenschaften für die Partition fest, für die sie gelten sollen.

internalIdLowerLimit

Beschreibung

Die Eigenschaften `internalIdUpperLimit` und `internalIdLowerLimit` beschränken die internen IDs von Campaign auf den angegebenen Bereich. Bitte berücksichtigen Sie, dass die Werte inklusiv zu verstehen sind: das heißt, Campaign kann sowohl die Unter- als auch die Obergrenze verwenden.

Standardwert

`0` (null)

internalIdUpperLimit

Beschreibung

Die Eigenschaften `internalIdUpperLimit` und `internalIdLowerLimit` beschränken die internen IDs von Campaign auf den angegebenen Bereich. Die Werte sind inklusiv zu verstehen: das heißt, Campaign kann sowohl die Unter- als auch die Obergrenze verwenden. Wenn Distributed Marketing installiert ist, setzen Sie den Wert auf `2147483647`.

Standardwert

`4294967295`

eMessageInstalled

Beschreibung

Gibt an, dass eMessage installiert ist. Wenn Sie `Yes` auswählen, sind eMessage-Funktionen in der Campaign-Schnittstelle verfügbar.

Das IBM Installationsprogramm setzt diese Eigenschaft für die Standardpartition in Ihrer eMessage-Installation auf `Yes`. Für weitere Partitionen, in denen Sie eMessage installiert haben, müssen Sie diese Eigenschaft manuell konfigurieren.

Standardwert

`Nein`

Gültige Werte

`Yes | No`

interactInstalled

Beschreibung

Nach der Installation der Interact-Gestaltungsumgebung sollte diese Konfigurationseigenschaft auf `Yes` gesetzt werden, um die Interact-Gestaltungsumgebung in Campaign zu aktivieren.

Falls Interact nicht installiert ist, auf `No` setzen. Durch Festlegen dieser Eigenschaft auf `No` werden die Interact-Menüs und -Optionen nicht aus der Benutzerschnittstelle entfernt. Wenn Sie die Menüs und Optionen entfernen möchten, müssen Sie die Registrierung von Interact unter Verwendung des Dienstprogramms `configTool` manuell aufheben.

Standardwert

No

Gültige Werte

Yes | No

Verfügbarkeit

Diese Eigenschaft ist nur anwendbar, wenn Interact installiert ist.

MO_UC_integration

Beschreibung

Ermöglicht die Integration mit Marketing Operations für diese Partition, sofern die Integration in den **Platform**-Konfigurationseinstellungen akti-

viert ist. Weitere Informationen finden Sie im Abschnitt *IBM Marketing Operations und im Campaign-Integrationshandbuch*.

Standardwert

No

Gültige Werte

Yes | No

MO_UC_BottomUpTargetCells

Beschreibung

Ermöglicht für diese Partition Bottom-up-Zellen für Arbeitsblätter für Zielzellen, sofern **MO_UC_integration** aktiviert ist. Ist dieser Wert auf `Yes` gesetzt, sind sowohl Top-down- als auch Bottom-up-Zielzellen sichtbar, die Bottom-up-Zielzellen sind jedoch schreibgeschützt. Weitere Informationen finden Sie im Abschnitt *IBM Marketing Operations und im Campaign-Integrationshandbuch*.

Standardwert

No

Gültige Werte

Yes | No

Legacy_campaigns

Beschreibung

Ermöglicht für diese Partition den Zugriff auf Kampagnen, die vor der Integration von Marketing Operations und Campaign erstellt wurden. Gilt nur, wenn **MO_UC_integration** auf `Yes` gesetzt ist. Veraltete Kampagnen umfassen auch Kampagnen, die in Campaign 7.x erstellt wurden und mit Plan 7.x-Projekten verbunden sind. Weitere Informationen finden Sie im Abschnitt *IBM Marketing Operations und im Campaign-Integrationshandbuch*.

Standardwert

No

Gültige Werte

Yes | No

IBM Marketing Operations – Angebotsintegration

Beschreibung

Bietet die Möglichkeit, Marketing Operations zu verwenden, um in dieser Partition Lifecycle-Management-Tasks für Angebote auszuführen, wenn für diese Partition **MO_UC_integration** aktiviert ist. In Ihren **Platform**-Konfigurationseinstellungen muss die Angebotsintegration aktiviert sein. Weitere Informationen finden Sie im Abschnitt *IBM Marketing Operations und im Campaign-Integrationshandbuch*.

Standardwert

No

Gültige Werte

Yes | No

UC_CM_integration

Beschreibung

Aktiviert die Digital Analytics-Onlinesegmentintegration für eine Campaign-Partition. Wenn Sie diesen Wert auf `Yes` setzen, bietet das Fenster "Select process" (Auswahlprozess) in einem Ablaufdiagramm die Option zur Auswahl von **Digital Analytics-Segmenten** als Eingabe. Wenn Sie die Digital Analytics-Integration für die einzelnen Partitionen ändern möchten, wählen Sie **Einstellungen > Konfiguration > Campaign | Partitionen | Partition[n] | Coremetrics**.

Standardwert

No

Gültige Werte

Yes | No

Campaign | Partitionen | Partition[n] | eMessage | contactAndResponseHistTracking

Mit den Eigenschaften in dieser Kategorie kann die eMessage-Angebotsintegration mit IBM Campaign für die aktuelle Partition konfiguriert werden.

etlEnabled

Beschreibung

Campaign verwendet den eigenen ETL-Prozess, um Antwortdaten zu Angeboten aus den eMessage-Verfolgungstabellen in die Campaign-Kontakttabellen und -Antwortverlaufstabellen zu extrahieren, zu transformieren und zu laden.

Der ETL-Prozess koordiniert Informationen aus den verschiedenen erforderlichen Tabellen, einschließlich `UA_UsrResponseType` (Campaign-Antworttypen) und `UA_RespTypeMapping` (Zuordnung von Antworttypen zwischen Campaign und eMessage).

Wird der Wert auf `Yes` gesetzt, wird sichergestellt, dass Informationen über Kontakte und Antwortverlauf in Verbindung mit eMessage-Angeboten zwischen Campaign und eMessage koordiniert werden. Beispielsweise werden E-Mail-Antwortdaten in Campaign-Berichte aufgenommen.

Anmerkung: Sie müssen darüber hinaus `Campaign | Partitionen | Partition[n] | Server | intern | eMessageInstalled` für diese Partition auf `Yes` setzen, da sonst der ETL-Prozess nicht ausgeführt wird.

Standardwert

`No`

Gültige Werte

`Yes | No`

runOnceADay

Beschreibung

Geben Sie an, ob der ETL-Prozess nur einmal am Tag ausgeführt werden sollte.

Falls der Wert Yes ist: Sie müssen **startTime** angeben. Der ETL-Job wird dann ausgeführt bis alle Datensätze verarbeitet sind und **sleepIntervalInMinutes** wird ignoriert.

Falls der Wert No ist: Der ETL-Job startet, sobald der Campaign-Web-Server startet. Der ETL-Job stoppt, nachdem alle Datensätze verarbeitet wurden, und wartet dann auf die von **sleepIntervalInMinutes** angegebene Zeit.

Standardwert

No

Gültige Werte

Yes | No

batchSize

Beschreibung

Der ETL-Prozess verwendet diesen Parameter, um Datensätze abzurufen, die von der RCT in die lokalen eMessage-Systemtabellen heruntergeladen wurden. Da sich große Werte auf die Leistung auswirken können, ist die Liste der verfügbaren Werte auf die nachstehend genannten gültigen Werte beschränkt. Falls Sie große Datenmengen erwarten, passen Sie **batchSize** zusammen mit **sleepIntervalInMinutes** an, um Datensätze in regelmäßigen Intervallen zu verarbeiten.

Standardwert

100

Gültige Werte

100 | 200 | 500 | 1000

sleepIntervalInMinutes

Beschreibung

Geben Sie das Intervall zwischen ETL-Jobs in Minuten an. Diese Option legt die Wartezeit nach dem Abschluss eines Jobs fest. Der ETL-Prozess setzt in diesem Zeitraum aus, bevor der nächste Job gestartet wird. Es können mehrere Jobs gleichzeitig ausgeführt werden und es kann mehrere ETL-Jobs in einer Partition geben.

Falls **runOnceADay** auf Yes gesetzt ist, kann kein Ruheintervall festgelegt werden.

Standardwert

60

Gültige Werte

Positive ganze Zahlen

startTime

Beschreibung

Geben Sie eine Zeit ein, zu der der ETL-Job gestartet werden soll. Sie müssen das englische Format verwenden, um die Startzeit anzugeben.

Standardwert

12:00:00 AM

Gültige Werte

Jede gültige Zeit im Format `hh:mm:ss AM/PM`

notificationScript

Beschreibung

Eine optionale ausführbare Datei oder Scriptdatei, die nach Abschluss eines ETL-Jobs ausgeführt wird. So möchten Sie vielleicht zu Überwachungszwecken über Erfolg oder Fehler eines ETL-Jobs benachrichtigt werden. Das Benachrichtigungsscript wird immer ausgeführt, wenn der ETL-Job für eine bestimmte Partition abgeschlossen wird.

Die an dieses Script übergebenen Parameter stehen fest und können nicht geändert werden. Das Script kann die folgenden Parameter verwenden:

- etlStart: Die Startzeit des ETL-Prozesses in Millisekunden.
- etlEnd: Die Endzeit des ETL-Prozesses in Millisekunden.
- totalCHRecords: Die Gesamtzahl der verarbeiteten Kontaktdokumente.
- totalRHRecords: Die Gesamtzahl der verarbeiteten Antwortverlaufsdokumente.
- executionStatus: Ausführungsstatus des ETL-Prozesses mit Wert 1 (fehlgeschlagen) oder 0 (erfolgreich).

Standardwert

Es ist kein Standardwert definiert.

Gültige Werte

Jeder gültige Pfad, auf den der Campaign-Server mit Lese- und Ausführungsberechtigung zugreifen kann. Beispiel: `D:\myscripts\scriptname.exe`

Zugehörige Konzepte:

„Unterstützung für die Integration von Campaign-Angeboten" auf Seite 47

eMessage | serverComponentsAndLocations | hostedServices

Sie können Eigenschaften definieren, über die die URLs zum Herstellen einer Verbindung zu IBM EMM Hosted Services angegeben werden. eMessage verwendet jeweils eigene Verbindungen zum Hochladen von Empfängerlisten und Metadaten, mit denen die Empfängerlisten beschrieben werden, und für die allgemeine Kommunikation, die an die gehostete Umgebung gesendet wird.

Wenn Sie eine Verbindung zu IBM EMM Hosted Services über das von IBM in Großbritannien eingerichtete Rechenzentrum herstellen, müssen Sie die Standardwerte ändern. Fragen Sie bei IBM an, mit welchem Rechenzentrum Sie verbunden sind.

uiHostName

Beschreibung

Die Adresse, die eMessage für die gesamte Kommunikation mit IBM EMM Hosted Services verwendet, ausgenommen dem Hochladen von Empfängerlisten und von zugehörigen Metadaten.

Standardwert

`em.unicaondemand.com`

Wenn Sie eine Verbindung zum Rechenzentrum in Großbritannien herstellen, müssen Sie diesen Wert in `em-eu.unicaondemand.com` ändern.

dataHostName

Beschreibung

Die Adresse, über die eMessage Metadaten (in Zusammenhang mit Empfängerlisten) in IBM EMM Hosted Services hochlädt.

Standardwert

`em.unicaondemand.com`

Wenn Sie eine Verbindung zum Rechenzentrum in Großbritannien herstellen, müssen Sie diesen Wert in `em-eu.unicaondemand.com` ändern.

ftpHostName

Beschreibung

Die Adresse, über die eMessage Empfängerlistendaten (mit Ausnahme von Listenmetadaten) in IBM EMM Hosted Services hochlädt.

Standardwert

`ftp-em.unicaondemand.com`

Wenn Sie eine Verbindung zum Rechenzentrum in Großbritannien herstellen, müssen Sie diesen Wert in `ftp-em-eu.unicaondemand.com` ändern.

eMessage | Partitionen | Partition[n] | hostedAccountInfo

In dieser Kategorie werden Eigenschaften definiert, um Benutzerberechtigungen für die Datenbank zu definieren, die die Kontoinformationen enthält, die für den Zugriff auf IBM EMM Hosted Services erforderlich sind. Die Werte, die Sie hier angeben, müssen in Marketing Platform als Benutzereinstellungen definiert sein.

amUserForAcctCredentials

Beschreibung

Verwenden Sie diese Eigenschaft, um den Marketing Platform-Benutzer anzugeben, der eine Marketing Platform-Datenquelle enthält, die die Berechtigungsnachweise für den Kontozugriff angibt, die für den Zugriff auf IBM EMM Hosted Services erforderlich sind.

Standardwert

asm_admin

Gültige Werte

Jeder Marketing Platform-Benutzer.

amDataSourceForAcctCredentials

Beschreibung

Verwenden Sie diese Eigenschaft, um die Marketing Platform-Datenquelle anzugeben, die die Anmeldeberechtigungsnachweise für IBM EMM Hosted Services definiert.

Standardwert

UNICA_HOSTED_SERVICES

Gültige Werte

Eine Datenquelle, die dem Benutzer zugeordnet ist, den Sie in `amUserForAcctCredentials` angeben.

eMessage | Partitionen | Partition[n] | dataSources | systemTables

Diese Kategorie enthält Konfigurationseigenschaften, die das Schema, Verbindungseinstellungen und Anmeldeberechtigungsnachweise für die Datenbank definieren, die die eMessage-Systemtabellen in Ihrer Netzumgebung enthält.

type

Beschreibung

Typ der Datenbank, die die eMessage-Systemtabellen hostet.

Standardwert

Es ist kein Standardwert definiert. Sie müssen diese Eigenschaft festlegen.

Gültige Werte

- `SQLSERVER`
- `ORACLE9`
- `ORACLE10` (wird auch verwendet, um Oracle 11-Datenbanken anzugeben)
- `DB2`

schemaName

Beschreibung

Name des Datenbankschemas für die eMessage-Systemtabellen. Dieser Name stimmt mit dem Schemanamen für die Campaign-Systemtabellen überein.

Sie müssen diesen Schemanamen angeben, wenn Sie in Scripts auf Systemtabellen verweisen.

Standardwert

dbo

jdbcBatchSize

Beschreibung

Die Anzahl an Ausführungsanforderungen, die JDBC zu einem bestimmten Zeitpunkt in der Datenbank ausführt.

Standardwert

10

Gültige Werte

Eine ganze Zahl größer als 0.

jdbcClassName

Beschreibung

Der JDBC-Treiber für Systemtabellen gemäß der Definition in Ihrem Campaign-Web-Server.

Standardwert

Es ist kein Standardwert definiert. Sie müssen diese Eigenschaft festlegen.

jdbcURI

Beschreibung

URI der JDBC-Verbindung für Systemtabellen gemäß der Definition in Ihrem Campaign-Web-Server.

Standardwert

Es ist kein Standardwert definiert. Sie müssen diese Eigenschaft festlegen.

asmUserForDBCredentials

Beschreibung

Verwenden Sie diese Eigenschaft, um einen IBM EMM-Benutzer anzugeben, der für den Zugriff auf die eMessage-Systemtabellen berechtigt ist.

Standardwert

Es ist kein Standardwert definiert. Sie müssen diese Eigenschaft festlegen.

Gültige Werte

Jeder in Marketing Platform definierte Benutzer. Dies sollte normalerweise der Name des Systembenutzers für Campaign sein.

amDataSourceForDBCredentials

Beschreibung

Verwenden Sie diese Eigenschaft, um die Datenquelle anzugeben, die Anmeldeberechtigungsnachweise für die Datenbank definiert, die die eMessage-Systemtabellen enthält. Diese kann mit der Datenquelle für die Campaign-Systemtabellen übereinstimmen.

Standardwert

UA_SYSTEM_TABLES

Gültige Werte

Eine Marketing Platform-Datenquelle, die dem IBM EMM-Benutzer zugeordnet ist, den Sie in `asmUserForDBCredentials` angeben.

Die Datenquelle gibt einen Datenbankbenutzer und die für den Zugriff auf die eMessage-Systemtabellen verwendeten Berechtigungsnachweise an. Wenn es sich bei dem Standardschema für den Datenbankbenutzer nicht um das Schema handelt, das die Systemtabellen enthält, müssen Sie das Systemtabellenschema in der JDBC-Verbindung angeben, die für den Zugriff auf die Systemtabellen verwendet wird.

poolAcquireIncrement

Beschreibung

Wenn es im Datenbankverbindungspool keine Verbindungen mehr gibt, die Anzahl neuer Verbindungen, die eMessage für die Systemtabellen erstellt. eMessage erstellt neue Verbindungen bis zu der in `poolMaxSize` angegebenen Anzahl.

Standardwert

1

Gültige Werte

Eine ganze Zahl größer als 0.

poolIdleTestPeriod

Beschreibung

Die Anzahl Sekunden, die eMessage zwischen Tests inaktiver Verbindungen zu den eMessage-Systemtabellen auf Aktivität wartet.

Standardwert

100

Gültige Werte

Eine ganze Zahl größer als 0.

poolMaxSize

Beschreibung

Die maximale Anzahl an Verbindungen von eMessage zu den Systemtabellen. Ein Wert von null (0) weist darauf hin, dass es keinen maximalen Wert gibt.

Standardwert

100

Gültige Werte

Eine ganze Zahl größer-gleich 0.

poolMinSize

Beschreibung

Die minimale Anzahl an Verbindungen von eMessage zu den Systemtabellen.

Standardwert

10

Gültige Werte

Eine ganze Zahl größer-gleich 0.

poolMaxStatements

Beschreibung

Die maximale Anzahl an Anweisungen, die eMessage im PrepareStatement-Cache pro Verbindung zu den Systemtabellen speichert. Wird poolMaxStatements auf null (0) gesetzt, wird das Anweisungscaching inaktiviert.

Standardwert

0

Gültige Werte

Eine ganze Zahl größer-gleich 0.

timeout

Beschreibung

Die Anzahl Sekunden, in denen eMessage eine inaktive Datenbankverbindung aufrechterhält, bevor die Verbindung unterbrochen wird.

Ist `poolIdleTestPeriod` größer als 0, testet eMessage alle `timeout` Sekunden alle inaktiven, zusammengefassten, aber nicht ausgecheckten Verbindungen.

Ist `poolIdleTestPeriod` größer als `timeout`, werden die inaktiven Verbindungen unterbrochen.

Standardwert

100

Gültige Werte

Eine ganze Zahl größer-gleich 0.

eMessage | Partitionen | Partition[n] | recipientListUploader

Diese Konfigurationskategorie enthält eine optionale Eigenschaft für die Position eines benutzerdefinierten Scripts, das als Reaktion auf die Aktionen oder den Status des Recipient List Uploaders ausgeführt wird.

pathToTriggerScript

Beschreibung

Sie können ein Script erstellen, das eine Aktion als Reaktion auf den Upload einer Empfängerliste an IBM EMM Hosted Services auslöst. Beispielsweise können Sie ein Script erstellen, um eine E-Mail-Benachrichtigung an den Listendesigner zu senden, wenn der Listenupload erfolgreich beendet wird.

Wenn Sie einen Wert für diese Eigenschaft definieren, leitet eMessage Statusinformationen über den Recipient List Uploader an die angegebene Position weiter. Wenn Sie diese Eigenschaft nicht angeben, wird eMessage nicht aktiv.

Standardwert

Es ist kein Standardwert definiert.

Gültige Werte

Jeder gültige Netzpfad.

eMessage | partitions | partition[n] | responseContactTracker

Eigenschaften dieser Kategorie geben das Verhalten des Response and Contact Tracker (RCT) an. Der RCT ruft für E-Mail-Kontakte, für die E-Mail-Zustellung und Empfängerantworten (wie beispielsweise Link-Klicks und Öffnungsrate) Daten ab und verarbeitet sie.

pauseCustomerPremisesTracking

Beschreibung

eMessage speichert Kontakt- und Antwortdaten in einer Warteschlange in IBM EMM Hosted Services. Über diese Eigenschaft können Sie den RCT anweisen, den Datenabruf aus IBM EMM Hosted Services vorübergehend

zu stoppen. Wenn die Verfolgung wieder aufgenommen wird, lädt der RCT die aufgelaufenen Daten herunter.

Standardwert

False

Gültige Werte

True | False

waitTimeToCheckForDataAvailability

Beschreibung

Der RCT überprüft in regelmäßigen Abständen, ob neue Daten in Zusammenhang mit E-Mail-Kontakten oder Empfängerantworten vorhanden sind. Über diese Eigenschaft können Sie angeben, in welchen Abständen (in Sekunden) der RCT IBM EMM Hosted Services auf neue Daten überprüft. Der Standardwert ist 300 Sekunden (d. h. alle 5 Minuten).

Standardwert

300

Gültige Werte

Eine ganze Zahl größer als 1.

perfLogInterval

Beschreibung

Über diese Eigenschaft können Sie angeben, wie oft der RCT Leistungsstatistikdaten in einer Protokolldatei aufzeichnet. Der Wert, den Sie hier eingeben, gibt die Anzahl der Datenerfassungen zwischen Protokolleinträgen an.

Standardwert

10

Gültige Werte

Eine ganze Zahl größer als 0.

enableSeparatePartialResponseDataTracking

Beschreibung

Diese Eigenschaft gibt an, ob eMessage auch partielle E-Mail-Antwortdaten an die Verfolgungstabellen in Ihrer lokalen eMessage-Installation weiterleitet.

In eMessage sind die Mailing-Instanz-ID und die Nachrichtenfolgenummer erforderlich, damit E-Mail-Antworten korrekt zugeordnet werden können. Wenn Sie die separate Verfolgung von partiellen Antwortdaten aktivieren, fügt eMessage die unvollständigen Antworten in separate Verfolgungsdateien ein, in denen Sie sie anzeigen oder weiter verarbeiten können.

Standardwert

True

Gültige Werte

True | False

enableExecutionHistoryDataTracking

Beschreibung

Über diese Eigenschaft wird angegeben, ob zusätzliche Daten zum Verlauf der Mailing-Ausführung aus IBM EMM Hosted Services heruntergeladen werden können.

Standardmäßig ist diese Eigenschaft auf **False** gesetzt, um das Herunterladen zusätzlicher Daten zu verhindern. Wenn Sie diese Eigenschaft auf **True** setzen, können Sie Daten zu Mailing-Ausführungen herunterladen, die in der Regel nicht in die eMessage-Systemtabellen aufgenommen werden. Sie können das Mailing- und Datenbankmanagement mithilfe dieser Zusatzinformationen automatisieren.

Diese Konfigurationseigenschaft ist standardmäßig ausgeblendet. Sie können sie in Ihrer lokalen eMessage-Installation anzeigen, indem Sie das Script `switch_config_visibility.bat` (im Verzeichnis `emessage\tools`) ausführen.

Der Zugriff auf die Daten zum Verlauf von Mailing-Ausführungen kann von IBM angefordert werden. Wenn Sie Zugriff auf zusätzliche Daten zum Verlauf von Mailing-Ausführungen benötigen, wenden Sie sich unter `eacctsvc@us.ibm.com` an Ihren IBM Ansprechpartner.

Standardwert

False

Gültige Werte

True | False

Kapitel 7. Konfigurationen für die Implementierung mobiler IBM Push-Benachrichtigungen

Marketiers können über IBM eMessage Push-Benachrichtigungen an mobile Apps senden. Zur Unterstützung dieser Aktivität müssen die Systemadministratoren eMessage für die Kommunikation mit den mobilen Apps und mobilen Geräten konfigurieren, an welche die Marketiers Benachrichtigungen senden. Die Administratoren müssen auch eine Liste der Positionen unterhalten, die für die Benachrichtigungszustellung nach Positions-Triggering verwendet werden, und Standardwerte konfigurieren, die die Marketiers zur Konfiguration von Push-Operationen für Benachrichtigungen verwenden können. Entwickler mobiler Apps modifizieren die Apps entsprechend für die Integration in eMessage und IBM Messaging-Systeme.

Wenn Sie eMessage so konfigurieren möchten, dass mobile Push-Benachrichtigungen unterstützt werden, muss IBM Campaign 9.1.0.2 Fixpack oder höher installiert sein.

Überblick über die Integration mobiler Apps in IBM Messaging-Systeme

Im Rahmen der Integration einer mobilen App in IBM Messaging-Systeme ist eine Reihe von Aktionen und Designaktivitäten unter Beteiligung verschiedener Systeme und Organisationen erforderlich. Hierzu gehören die Kommunikation mit IBM Account Services, die Konfiguration von IBM eMessage sowie die Änderung Ihrer mobilen App mit einem SDK von IBM.

Bevor Sie beginnen, müssen Sie einige Vorbereitungen treffen, die von Apple und Google für Anwendungen verlangt werden, die in ihre jeweiligen Betriebssysteme für mobile Geräte und in ihre Benachrichtigungssysteme integriert werden.

In der Tabelle sind die erforderlichen Aktionen für die Integration einer mobilen App in die IBM Messaging-Services aufgeführt.

Folge	Aktivität	Informationen
1	Registrieren Sie Ihre mobile App bei Google Cloud Messaging oder dem Apple Push Notification Service.	„Voraussetzungen für die Integration von Google Android-Apps in IBM Push-Benachrichtigungen" auf Seite 64 „Voraussetzungen für die Integration von Apple iOS-Apps in IBM Push-Benachrichtigungen" auf Seite 76
2	Fordern Sie bei IBM die Aktivierung Ihres gehosteten Messaging-Kontos für mobiles Messaging an.	„Gehostetes Messaging-Konto für mobiles Messaging aktivieren" auf Seite 89
3	Registrieren Sie Ihre App bei IBM eMessage.	„Mobile App in IBM eMessage registrieren" auf Seite 90

© Copyright IBM Corp. 1999, 2015

Folge	Aktivität	Informationen
4	Bearbeiten Sie Ihre App für die Verwendung von IBM Push-Benachrichtigungen.	„IBM Push Notification SDK for Android in Ihrer App implementieren" auf Seite 65 „iOS in Ihrer App implementieren" auf Seite 76
5	Konfigurieren Sie Positionen für die Zustellung von Benachrichtigungen nach Positions-Triggering.	„Positionen für die Zustellung nach Positions-Triggering konfigurieren" auf Seite 93
6	Fordern Sie bei IBM die Aktivierung des automatischen Austauschs der Ergebnisse der Benachrichtigungsverfolgung an.	„Push-Benachrichtigung-Aufzeichnungsdaten von IBM" auf Seite 95

Integration von Google Cloud Messaging in IBM eMessage

IBM eMessage bietet eine einfache Möglichkeit der Integration von GCM-Push-Benachrichtigungen (GCM = Google Cloud Messaging) in Ihre Anwendungen für Android 2.2 und höher.

Zur GCM-Integration in IBM Messaging-Services müssen Sie das IBM Push-Benachrichtigungs-SDK für Android herunterladen und integrieren.

Zugehörige Konzepte:

„Voraussetzungen für die Integration von Google Android-Apps in IBM Push-Benachrichtigungen"

Zugehörige Tasks:

„Mobile App in IBM eMessage registrieren" auf Seite 90

Voraussetzungen für die Integration von Google Android-Apps in IBM Push-Benachrichtigungen

Bevor Sie mit der Integration einer mobilen Google Android-App in IBM Services für Push-Benachrichtigungen beginnen, müssen Sie Ihre mobile App für Android 2.2 und höher bei Google Cloud Messaging (GCM) registrieren und bereitstellen. Bei der Registrierung erstellen Sie ein GCM-Projekt. Zu jedem Projekt gibt es einen Paketnamen und eine Google-API-Projektnummer. Der Paketname und die API-Projektnummer müssen bei der Registrierung der mobilen App bei IBM Messaging-Services eingegeben werden.

Sie können separate Projekte für Entwicklungs- und Produktionsumgebungen erstellen. Bei der Registrierung der App bei den IBM Messaging-Services werden die Entwicklungs- und Produktionsprojekte separat registriert.

Die Registrierung und Bereitstellung Ihrer mobilen App bei GCM umfasst die folgenden Aktivitäten:

- Erstellen Sie einen Google-Messaging-Account.
- Richten Sie Google Play Services ein.
- Erstellen Sie ein Google-API-Projekt.
- Erstellen Sie Ihre App in Eclipse oder in der Befehlszeile.

- Registrieren Sie die App bei Google Cloud Messaging.
- Notieren Sie die Google-API-Projektnummer und den Google-API-Schlüssel. Diese Angaben werden zur Integration der App in eMessage und IBM Messaging-Systeme benötigt.

Beachten Sie unter Google (http://developer.android.com/google/gcm/index.html) die spezifischen Anleitungen zum Erstellen von Entwicklungs- und Produktionsprojekten in GCM.

Anmerkung: Achten Sie darauf, für jedes erstellte GCM-Projekt die Google-API-Projektnummer und den Google-API-Schlüssel aufzuzeichnen. Diese Werte müssen Sie bei der Registrierung der App bei IBM angeben.

Zugehörige Konzepte:

„Integration von Google Cloud Messaging in IBM eMessage" auf Seite 64

Zugehörige Tasks:

„Mobile App in IBM eMessage registrieren" auf Seite 90

IBM Push Notification SDK for Android in Ihrer App implementieren

Wenn Sie Google Cloud Messaging (GCM) in IBM Messaging-Services integrieren möchten, müssen Sie das IBM Push Notification SDK for Android herunterladen und Ihrer mobilen App hinzufügen. Ändern Sie das SDK und die mobile App, um die Benachrichtigungsfunktionen bereitzustellen, die IBM eMessage unterstützt.

Vorbereitende Schritte

Bevor Sie Ihre App ändern, um sie zusammen mit eMessage und IBM Messaging-Systemen einzusetzen, sind folgende Maßnahmen zu ergreifen.

- Registrieren Sie Ihre App für Google Cloud Messaging. Sie müssen die Google-API-Projektnummer und den Google-API-Schlüssel erfassen. Diese Werte sind für die Implementierung des SDK erforderlich.
- Registrieren Sie die App für eMessage. Im Rahmen des Registrierungsprozesses wird ein App-Schlüssel generiert. Der App-Schlüssel ist für die Implementierung des SDK erforderlich.

Informationen zu diesem Vorgang

Anmerkung: Weitere Anweisungen im Zusammenhang mit der Implementierung von IBM Push-Benachrichtigungen in Ihrer mobilen App finden Sie in der Beispiel-App, die zusammen mit dem IBM Push Notification SDK for Android bereitgestellt wird.

1. Laden Sie das IBM Push Notification SDK for Android Version 2.x von IBM developerWorks unter https://www.ibmdw.net/push/docs/ibm-mobile-push-notification/google-cloud-messaging/download-ibm-push-notification-sdk-android/ herunter.
2. Fügen Sie Ihrem Projektpfad IBM Push Notification SDK for Android hinzu.
   a. Erstellen Sie in Ihrem Projekt einen neuen Ordner mit dem Namen `libs` und verschieben Sie die JAR-Datei des IBM Push Notification SDK for Android in diesen Ordner. Suchen Sie die SDK-JAR-Datei im Stammverzeichnis, nachdem Sie das SDK-Paket extrahiert haben.

b. Wählen Sie Ihr Projekt aus.
c. Klicken Sie mit der rechten Maustaste auf **Eigenschaften**.
d. Wählen Sie **java build path** (Java-Buildpfad) aus.
e. Klicken Sie auf die Registerkarte **libraries** (Bibliotheken).
f. Wählen Sie **Add JARs** (JARs hinzufügen) aus und navigieren Sie zur IBM Push Notification SDK for Android-JAR-Datei im libs-Ordner.

3. Ändern Sie die Datei `AndroidManifest.xml`.
   a. Android-Version: Setzen Sie die Android SDK-Version mindestens auf '8' (Android 2.2) oder höher. Das IBM Push Notification SDK for Android funktioniert nicht mit Vorgängerversionen.

      ```
      <uses-sdk android:minSdkVersion="8" />
      ```

   b. Berechtigungen: Die folgenden Berechtigungen werden benötigt, damit das SDK ordnungsgemäß funktioniert. Diese Berechtigungen werden als untergeordnetes Element des `<Manifest>`-Knotens positioniert. Ersetzen Sie die beiden Vorkommen von `NAME_IHRES_APP-PAKETS` durch den Namen Ihres Anwendungspakets.

```
<permission android:name="NAME_IHRES_APP-PAKETS.permission.C2D_MESSAGE"
                android:protectionLevel="signature" />
  <uses-permission android:name="NAME_IHRES_APP-PAKETS.permission.C2D_MESSAGE" />
  <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE" />
  <uses-permission android:name="android.permission.INTERNET" />
  <uses-permission android:name="android.permission.WAKE_LOCK" />
  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
```

      Wenn Sie die optionale Anwahloption (Dial Action) auf der Seite mit Details zu Benachrichtigungen verwenden möchten, müssen Sie die folgenden Informationen hinzufügen:

      ```
      <uses-permission android:name="android.permission.CALL_PHONE" />
      ```

   c. Anwendungskomponenten: Fügen Sie dem `<Anwendungs>`-Knoten die folgende xml-Datei hinzu. Ersetzen Sie die Vorkommen von `NAME_IHRES_APP-PAKETS` durch den Namen Ihres Anwendungspakets.

```
<provider
  android:name="com.xtify.sdk.db.Provider"
  android:authorities="NAME_IHRES_APP-PAKETS.XTIFY_PROVIDER"
  android:exported="false" />
<receiver android:name="com.xtify.sdk.c2dm.C2DMBroadcastReceiver" >
 <intent-filter android:permission="com.google.android.c2dm.permission.SEND" >
  <action android:name="com.google.android.c2dm.intent.RECEIVE" />
  <category android:name="NAME_IHRES_APP-PAKETS" />
 </intent-filter>
 <intent-filter android:permission="com.google.android.c2dm.permission.SEND" >
  <action android:name="com.google.android.c2dm.intent.REGISTRATION" />
  <category android:name="NAME_IHRES_APP-PAKETS" />
 </intent-filter>
</receiver>

<receiver android:name="com.xtify.sdk.NotifActionReceiver" />
<receiver android:name="com.xtify.sdk.wi.AlarmReceiver" >
 <intent-filter>
  <action android:name="android.intent.action.BOOT_COMPLETED" />
 </intent-filter>
 <intent-filter>
  <action android:name="android.intent.action.TIMEZONE_CHANGED" />
 </intent-filter>
 <intent-filter>
  <action android:name="android.intent.action.PACKAGE_REPLACED" />
  <data android:scheme="package" />
 </intent-filter>
</receiver>
```

```
<service android:name="com.xtify.sdk.location.LocationUpdateService" />
<service android:name="com.xtify.sdk.c2dm.C2DMIntentService" />
<service android:name="com.xtify.sdk.alarm.MetricsIntentService" />
<service android:name="com.xtify.sdk.alarm.TagIntentService" />
<service android:name="com.xtify.sdk.alarm.RegistrationIntentService" />
<service android:name="com.xtify.sdk.alarm.LocationIntentService" />
```

4. Bearbeiten Sie Ihre Hauptaktivität: Führen Sie in Ihrer Hauptaktivität (der Aktivität, die gestartet wird, wenn die App zum ersten Mal geöffnet wird) Folgendes durch.
   a. Fügen Sie den folgenden Import hinzu:
      ```
      import com.xtify.sdk.api.XtifySDK;
      ```
   b. Rufen Sie dann in der onStart-Methode der Aktivität `XtifySDK.start` auf:

```
final String XTIFY_APP_KEY = "IHR_XTIFY_APP-SCHLÜSSEL";
final String PROJECT_NUM = "IHRE_PROJEKTNR"; // Dies ist die Google-Projektnummer
XtifySDK.start(getApplicationContext(), XTIFY_APP_KEY, PROJECT_NUM);
```

   Ersetzen Sie "IHR_XTIFY_APP-SCHLÜSSEL" durch Ihren IBM Mobile Push Notification appKey und "IHRE_PROJEKTNR" durch Ihre Google-API-Projektnummer.

   XtifySDK.start() startet den Registrierungsprozess für IBM Mobile Push Notification und GCM und stellt dann sicher, dass die Komponente IBM Push Notification SDK for Android ausgeführt wird.

```
public class MainActivity extends Activity {
    private static final String XTIFY_APP_KEY = "1234567-abcd-efgh-ijkl-25d2389b0178";
    private static final String PROJECT_NUM = "1234567890123";

    @Override
    protected void onStart() {
        super.onStart();
        XtifySDK.start(getApplicationContext(), XTIFY_APP_KEY, PROJECT_NUM);
    }
}
```

Lassen Sie nicht zu, dass Ihre App auf externen Speicherkarten installiert wird. Weitere Informationen erhalten Sie auf der Google Developer Site unter http://developer.android.com/guide/topics/data/install-location.html#ShouldNot. Stellen Sie sicher, dass die App auf internem Speicher installiert wird.

Einen App-Eingang für Android-Apps bereitstellen

Wenn Sie den Versand von Eingangsbenachrichtigungen an eine mobile Android-App unterstützen möchten, müssen Sie in der mobilen App einen Eingang erstellen, um sie zu empfangen.

Informationen zu diesem Vorgang

Im SDK von Android 2.x werden das Management von Eingangsbenachrichtigungen und der Eingang aus dem SDK entnommen, damit Sie die Ansicht für Ihre Anwendung anpassen können. Eingangsbenachrichtigungen werden manchmal auch als erweiterte Benachrichtigungen bezeichnet.

Vorgehensweise

1. Fügen Sie Ihrer App das Eingangsbenachrichtigungspaket hinzu.
   a. Erstellen Sie ein Klassenpaket mit dem Namen `com.xtify.rn`.
   b. Kopieren Sie aus dem Paket IBM Push Notification SDK for Android den Quellcode aus `Rich Notification/src/com/xtify/rn` in das neu erstellte Paket.

c. Kopieren Sie aus dem Paket IBM Push Notification SDK for Android den Inhalt des Ordners `Rich Notification/res/` in Ihren Projektordner `/res`.

2. Fügen Sie dem Anwendungsknoten im Manifest Folgendes hinzu.

```
<activity android:configChanges="orientation"
          android:name="com.xtify.rn.RichNotifInboxActivity"></activity>
<activity android:configChanges="orientation"
          android:name="com.xtify.rn.RichNotifActivity"></activity>
```

3. Fügen Sie in der Unterklasse "XtifyBroadcastReceiver" (XtifyNotifier in der Beispiel-App) den folgenden Methodenaufruf in "onMessage" hinzu.

```
import com.xtify.rn.RichNotificationManger;

public class XtifyNotifier extends XtifyBroadcastReceiver {

  ...

  @Override
  public void onMessage(Context context, Bundle msgExtras) {
    RichNotificationManger.processNotifExtras(context, msgExtras);

    ...
 }

 ...

 }
```

4. Um den Benachrichtigungseingang anzuzeigen, starten Sie `RichNotifInboxActivity`, indem Sie den folgenden Code in die onClick-Funktion Ihres Menüelements oder der Schaltfläche positionieren.

```
Intent intent = new Intent(this, RichNotifInboxActivity.class);
context.startActivity(intent);
```

   Wobei der Kontext der Aktivitätskontext ist. Sie können den Kontext abrufen, indem Sie in der Aktivität `this` verwenden.

Positionsgesteuerte Benachrichtigungen für Android-Apps bereitstellen

Wenn Sie den IBM Push Notification SDK for Android in die mobile App integrieren, kann die App nach Positionsaktualisierungen von mobilen Geräten suchen und diese an IBM Messaging-Services weiterleiten. Wenn sich ein mobiles Gerät innerhalb eines angegebenen Radius einer vordefinierten Position bewegt, sendet das System automatisch eine Benachrichtigung an den mobilen Benutzer.

Informationen zu diesem Vorgang

Das IBM Push Notification SDK for Android verwendet Netzadressdaten des NETZBETREIBER-Diensts, um Auswirkungen auf die Akkuleistung zu minimieren. Dieser Betreiber legt die Position fest, die auf der Verfügbarkeit von Mobilfunkmasten und WiFi-Zugangspunkten basiert. Ergebnisse werden nur unter Verwendung einer Netzsuche abgerufen, es wird kein GPS verwendet.

Wenn Sie permanente Überwachung und Aktualisierungen aktivieren, wird die Geräteposition alle 15 Minuten an IBM gesendet, selbst wenn die Anwendung im Hintergrund ausgeführt wird.

Vorgehensweise

1. Permanente Positionsüberwachung und -aktualisierungen aktivieren.

Der Kontext ist der Anwendungskontext. Sie können den Kontext durch Aufrufen von "Activity.getApplicationContext()" oder "Context.getApplicationContext()" abrufen.

a. Importieren Sie die Klasse "XtifyLocation".

```
import com.xtify.sdk.api.XtifyLocation;
```

b. Rufen Sie die folgende statische Methode in Ihrer Anwendung auf.

```
XtifyLocation.enableRepetitiveLocUpdate(context);
```

So können Sie die Funktion inaktivieren.

```
XtifyLocation.disableRepetitiveLocUpdate(context);
```

2. Aktualisieren Sie Ihr Manifest, um die folgende Berechtigung hinzuzufügen. Diese wird als untergeordnetes Element des `<Manifest>`-Knotens positioniert.

```
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
```

Zugehörige Tasks:

„Positionen für die Zustellung nach Positions-Triggering konfigurieren" auf Seite 93

Verfügbarkeit von Standortaktualisierungen auf Anfrage konfigurieren

Sie können Ihre mobile App so konfigurieren, dass Standortaktualisierungen an einem bestimmten Punkt in der Anwendung oder auf Benutzeranfrage zur Verfügung stehen. Die Standortaktualisierung kann beispielsweise auf eine Benutzeraktion hin erfolgen, zum Beispiel, wenn sich der Benutzer bei der App anmeldet.

Vorgehensweise

Verwenden Sie folgende Methode aus der Klasse `XtifyLocation`.

```
updateLocation(int timeOut, LocationUpdateListener locationUpdateListener);
```

Diese Methode hört so lange auf Standortaktualisierungen, bis der Standort bereitgestellt oder das Zeitlimit überschritten wird. Die Methode garantiert keine Standortzustellung an IBM. Die bereitgestellte `LocationUpdateListener`-Methode wird nur bei Empfang des Standorts aufgerufen. Eventuell müssen Sie eine Logik erstellen, um bei Fehlerbedingungen wie einer Zeitlimitüberschreitung die Verbindung wiederherzustellen.

Benutzerdefinierte Standortaktualisierungen konfigurieren

Zur Ermittlung des Standorts eines mobilen Geräts und zum anschließenden Senden der Benachrichtigung an IBM können Sie eine eigene Logik implementieren.

Vorgehensweise

Verwenden Sie folgende Methode aus der Klasse `XtifyLocation`.

```
updateLocation(int timeOut, LocationUpdateListener locationUpdateListener);
```

Diese Methode garantiert keine Standortzustellung an IBM. Die bereitgestellte `LocationUpdateListener`-Methode wird nur bei Empfang des Standorts aufgerufen. Eventuell müssen Sie eine Logik erstellen, um bei Fehlerbedingungen wie einer Zeitlimitüberschreitung die Verbindung wiederherzustellen.

Beispiel

Nachfolgend ein möglicher Entwurf für benutzerdefinierte Standortaktualisierungen.

```
import com.xtify.sdk.api.XtifyLocation;
import com.xtify.sdk.api.XtifyLocation.LocationUpdateListener;

...

int timeOut = 2 * 60 * 1000; // one min
XtifyLocation xtifyLocation = new XtifyLocation(getApplicationContext());
xtifyLocation.updateLocation(timeOut, new LocationUpdateListener() {

  @Override
  public void onUpdateComplete(boolean result, Location location) {

  }

});

...
```

Benachrichtigungen zu Aktionszielen bereitstellen

Wenn Sie eine Aktivität unter Verwendung der Benachrichtigungsaktion `Action Intent` (Aktionsziel) öffnen möchten, müssen Sie den Aktivitätsknoten in der Datei `AndroidManifest.xml` aktualisieren.

Vorgehensweise

1. Fügen Sie dem Aktivitätsknoten in der Datei `AndroidManifest.xml` Folgendes hinzu.

   ```
   <intent-filter>
    <action android:name="com.yoursite.YOUR_ACTION_NAME" />
    <category android:name="android.intent.category.DEFAULT" />
   </intent-filter>
   ```

2. Ersetzen Sie `com.yoursite.YOUR_ACTION_NAME` durch Ihren Aktionsnamen. Wenn Sie eine Benachrichtigung über die Konsole senden, können Sie für "Action Intent" Ihren Aktionsnamen verwenden.

Unterstützung für Ereignisse und Benachrichtigungen konfigurieren

Verwenden Sie das IBM Push Notification SDK, um auf Ereignisse und eingehende Benachrichtigungs-Push-Daten zu reagieren.

Informationen zu diesem Vorgang

1. Fügen Sie dem Anwendungsknoten im Manifest Folgendes hinzu:

   ```
   <receiver android:name=".XtifyNotifier" >
    <intent-filter>
     <action android:name="com.xtify.sdk.NOTIFIER" />
    </intent-filter>
   </receiver>
   ```

2. Erstellen Sie eine Klasse, benennen Sie sie in Ihrem Hauptpaket mit `XtifyNotifier` und verwenden Sie folgenden Code als Inhalt dieser neuen Klassendatei:

   ```
   import android.content.Context;
   import android.os.Bundle;
   import com.xtify.sdk.api.XtifyBroadcastReceiver;
   ```

```
public class XtifyNotifier extends XtifyBroadcastReceiver {

 @Override
 protected void onMessage(Context context, Bundle msgExtras){
 }

 @Override
 protected void onRegistered(Context context) {
 }

 @Override
 protected void onC2dmError(Context context, String errorId) {
 }

}
```

Die Methoden in `XtifyNotifier` werden aufgerufen, selbst wenn Ihre Anwendung nicht ausgeführt wird (siehe Anmerkungen zu XtifyNotifier). Nachstehend eine Erläuterung, welche Ergebnisse Sie mit den einzelnen Methoden erzielen und wann.

1. onMessage: Die Nachrichtenzusatzinformationen werden in onMessage im Bundle-Parameter empfangen. Sie können die Zusatzinformationen im vorherigen Beispiel abrufen, indem Sie die Zeichenfolgen nach Schlüssel abrufen:

   ```
   msgExtras.getString(key);
   ```

   Der Schlüssel kann einer der folgenden sein.

   a. Ein in IBM Push-Benachrichtigungen festgelegter Schlüssel.

Tabelle 1. Schlüsseltabelle.

Schlüssel	Beschreibung
com.xtify.sdk.NOTIFICATION_TITLE	Titel der einfachen Benachrichtigung.
com.xtify.sdk.NOTIFICATION_CONTENT	Inhalt der einfachen Benachrichtigung.
com.xtify.sdk.NOTIF_ACTION_TYPE	Der Typ der Aktion, der in IBM Push Notification zur Ausführung durch das SDK festgelegt wurde. (Beispielsweise `com.xtify.sdk.OPEN_URL`)
com.xtify.sdk.NOTIF_ACTION_DATA	Daten, die sich auf den Aktionstyp beziehen (z. B. bei Open URL handelt es sich bei den Daten um die Website-URL).

   b. Ein angepasster Schlüssel, den Sie in den Nutzdaten festlegen (Sie können beispielsweise das Nutzdatenfeld in der Push-API oder in der App der Webkonsole wie folgt festlegen).

      Sie können den Wert in onMessage durch folgenden Aufruf abrufen:

      In diesem Fall ist der Rückgabewert "myValue".

      Anmerkung: Bei angepassten Schlüsseln (nicht bei IBM Push Notification-Schlüsseln) hat der Schlüssel das Präfix `data`.

2. onC2dmError: Wenn bei der Registrierung ein Fehler auftrat, wird onC2dmError mit einer Fehler-ID aufgerufen:

Tabelle 2. Fehlercodetabelle

Fehlercode	Beschreibung
SERVICE_NOT_AVAILABLE	Der Server gab 500/503 zurück. Das SDK versucht eine erneute Registrierung.

Tabelle 2. Fehlercodetabelle (Forts.)

Fehlercode	Beschreibung
ACCOUNT_MISSING	Auf dem Telefon gibt es kein Google-Konto. Die Anwendung sollte den Benutzer dazu auffordern, den Account-Manager zu öffnen und ein Google-Konto hinzuzufügen. Fix auf der Geräteseite.
AUTHENTICATION_FAILED	Ungültiges Kennwort. Die Anwendung sollte den Benutzer dazu auffordern, sein Kennwort einzugeben, und es ihm ermöglichen, es später manuell erneut zu versuchen. Fix auf der Geräteseite.
TOO_MANY_REGISTRATIONS	Der Benutzer hat zu viele Anwendungen registriert. Die Anwendung sollte den Benutzer dazu auffordern, einige andere Anwendungen zu deinstallieren, und es ihm ermöglichen, es manuell erneut zu versuchen. Fix auf der Geräteseite.
INVALID_SENDER	Das Absenderkonto wird nicht erkannt.
PHONE_REGISTRATION_ERROR	Falsche Telefonregistrierung bei Google. Dieses Telefon unterstützt GCM derzeit nicht.

3. onRegister: Diese Methode wird aufgerufen, wenn IBM Push Notification SDK for Android bei IBM und GCM registriert wird und bereit ist, Benachrichtigungen zu empfangen. Wenn Sie die XID des Benutzers abrufen und dauerhaft in Ihrer Benutzertabelle speichern möchten, sollten Sie das hier tun.

Nächste Schritte

XtifyNotifier extends XtifyBroadcastReceiver, eine Unterklasse von android.content-.BroadcastReceiver. Die abstrakten Methoden in XtifyNotifier werden von BroadcastReceiver.onReceive aufgerufen. Sie haben denselben Lebenszyklus wie alle BroadcastReceiver. Weitere Informationen finden Sie im Abschnitt http://developer.android.com/reference/android/content/BroadcastReceiver.html#ReceiverLifecycle.

Die Bibliothek überträgt ein Ziel durch einfaches Klicken auf "com.xtify.sdk.EVENT_NCK". Sie können in Ihrem Projekt einen Empfänger einrichten und im Falle einer Aktion eine angepasste Logik ausführen, z. B. Übergabe des Klicks an Google Analytics SDK. So erfolgt die Einrichtung.

1. Erstellen Sie eine Klasse mit dem Namen "XtifyEventReceiver", fügen Sie den nachstehenden Code hinzu und ersetzen Sie ANGEPASSTER_CODE durch Ihren Code, der auf einen Klick reagiert:

```
public class XtifyEventReceiver extends BroadcastReceiver {
  @Override
  public void onReceive(Context context, Intent intent) {

    if(intent.getAction() == "com.xtify.sdk.EVENT_NCK"){
      Log.i(XtifyEventReceiver.class.getName(), "Notification clicked.");
      ANGEPASSTER_CODE
    }
  }
}
```

2. Fügen Sie Ihrer Manifestdatei Folgendes hinzu und ersetzen Sie NAME_IHRES_PAKETS durch den Paketnamen, der die Klasse XtifyEventReceiver enthält:

```
<receiver android:name="NAME_IHRES_PAKETS.XtifyEventReceiver" >
 <intent-filter>
  <action android:name="com.xtify.sdk.EVENT_NCK" />
 </intent-filter>
</receiver>
```

Anmerkung: Sollte es im Rahmen Ihres Anwendungsfalls notwendig sein, müssen Sie ggf. eine App Open-Metrik (offene App) erfassen. Wenn Sie beispielsweise im Rahmen einer angepassten Aktion Deep-Drops in Ihrer Anwendung bearbeiten, können Sie einen App Open-Status protokollieren, indem Sie Folgendes aufrufen:

```
XtifyMetricsManager.addMetric(context, MetricAction.APP_OPENED,
        "<Insert ISO8601 time string>");
```

Benachrichtigungen anpassen

Sie können das Verhalten von Standardbenachrichtigungen anpassen, indem Sie die Klasse `com.xtify.sdk.api.NotificationsPreference` im IBM Push Notification SDK for Android verwenden.

Tonsignale für Benachrichtigungen aktivieren und ändern

Wenn Sie ein Tonsignal für die Benachrichtigungen Ihrer mobilen App abspielen möchten, müssen Sie die Klasse NotificationsPreference ändern.

Vorgehensweise

1. Wenn Sie ein Tonsignal für Benachrichtigungen aktivieren möchten, rufen Sie die folgende statische Methode aus der Klasse NotificationsPreference auf:

   ```
   NotificationsPreference.setSoundEnabled(context, true);
   ```

2. Wenn Sie das Tonsignal für Benachrichtigungen ändern möchten, nehmen Sie zuerst Ihre Audiodatei in den Ordner `/res/raw/` in Ihrem Projekt auf und rufen Sie dann die statische Methode `NotificationsPreference.setSound(context,soundResourceID)` auf. Beispiel:

   ```
   NotificationsPreference.setSound(context, R.raw.notification_sound);
   ```

   Anmerkung: Wenn Sie ein Tonsignal aktiviert, jedoch kein angepasstes Tonsignal festgelegt haben, wird das Standardtonsignal des Systems verwendet.

Vibrationssignale für Benachrichtigungen aktivieren und ändern

Wenn Sie Vibrationssignale für die Benachrichtigungen Ihrer mobilen App aktivieren oder ändern möchten, müssen Sie `AndroidManifest.xml` und die Klasse NotificationsPreference ändern.

Vorgehensweise

1. Wenn Sie ein Vibrationssignal für Benachrichtigungen aktivieren möchten, fügen Sie der Datei `AndroidManifest.xml` folgende Berechtigung hinzu:

   ```
   <uses-permission android:name="android.permission.VIBRATE"/>
   ```

2. Rufen Sie dann die folgende statische Methode aus der Klasse NotificationsPreference auf:

   ```
   NotificationsPreference.setVibrateEnabled(context, true);
   ```

3. Wenn Sie das Vibrationsmuster für Benachrichtigungen ändern möchten, rufen Sie die statische Methode NotificationsPreference.setVibrationPattern(context,vibrationPattern) auf. Beispiel:

   ```
   long [] vibrate = {0,100,200,300};
   NotificationsPreference.setVibrationPattern(context,vibrate);
   ```

Anmerkung: Wenn Sie ein Vibrationssignal aktiviert, jedoch kein angepasstes Vibrationsmuster festgelegt haben, wird das Standardvibrationsmuster des Systems verwendet.

Symbolsignale für Benachrichtigungen aktivieren und ändern

Wenn Sie Symbolsignale für die Benachrichtigungen Ihrer mobilen App aktivieren oder ändern möchten, müssen Sie die Klasse NotificationsPreference ändern.

Vorgehensweise

Wenn Sie das Symbolsignal für Benachrichtigungen ändern möchten, rufen Sie die statische Methode NotificationsPreference.setIcon(context,iconResourceID) auf. Beispiel:

```
NotificationsPreference.setIcon(context, R.drawable.notification_icon);
```

Anmerkung: Das Standardssymbolsignal für Benachrichtigungen ist android.R.drawable.sym_def_app_icon.

Lichtsignale für Benachrichtigungen aktivieren und ändern

Wenn Sie Lichtsignale für die Benachrichtigungen Ihrer mobilen App aktivieren oder ändern möchten, müssen Sie die Klasse NotificationsPreference ändern.

Vorgehensweise

1. Wenn Sie Lichtsignale für Benachrichtigungen aktivieren möchten, rufen Sie die folgende statische Methode aus der Klasse NotificationsPreference auf.

   ```
   NotificationsPreference.setLightsEnabled(context, true);
   ```

2. Wenn Sie die Vorgaben für die Lichtsignale für Benachrichtigungen ändern möchten, rufen Sie die statische Methode NotificationsPreference.setLights(getApplicationContext(), new int[] { ledARGB , ledOnMS , ledOffMS }); auf. Beispiel:

```
int ledARGB = 0x00a2ff;
int ledOnMS = 300;
int ledOffMS = 1000:
NotificationsPreference.setLights(getApplicationContext(), new int[] { ledARGB, ledOnMS, ledOffMS });
```

Anmerkung: Wenn Sie einer der Setter-Methoden in der Klasse NotificationsPreference eine Null übergeben, wird die Vorgabe zurückgesetzt und für neue Benachrichtigungen wird der Standardwert angewendet.

Flag-Benachrichtigungen aktivieren und ändern

Wenn Sie Flag-Benachrichtigungen für die Benachrichtigungen Ihrer mobilen App aktivieren oder ändern möchten, müssen Sie die Klasse NotificationsPreference ändern.

Vorgehensweise

Wenn Sie Benachrichtigungsflags für Benachrichtigungen hinzufügen möchten, rufen Sie die statische Methode NotificationsPreference.addFlags(context, NOTIFICATION_FLAG_1 | NOTIFICATION_FLAG_2); auf. Beispiel:

```
NotificationsPreference.addFlags(context, Intent.FLAG_ACTIVITY_SINGLE_TOP);
```

Anmerkung: Die Standardbenachrichtigungsflags sind FLAG_ACTIVITY_NEW_TASK und FLAG_ACTIVITY_CLEAR_TOP.
Alle Flags sind mit FLAG_ACTIVITY_NEW_TASK verbunden.
Weitere Informationen über Flags finden Sie im Abschnitt http://

developer.android.com/reference/android/content/Intent.html#FLAG_ACTIVITY_NEW_TASK.

Die Benutzer-ID einer mobilen App (XID) für Android integrieren

Bei der Benutzer-ID einer mobilen App handelt es sich um eine eindeutige ID, die das System jedem einzelnen Benutzer einer mobilen Anwendung zuweist, wenn dieser Ihre mobile App herunterlädt und installiert. Die Benutzer-ID einer mobilen App wird auch als XID bezeichnet. IBM Messaging-Systeme senden die Benutzer-ID einer mobilen App an das mobile Gerät. Sie müssen Ihre mobile Android-App konfigurieren, um die ID abzurufen und in der Marketing-Datenbank zur Nutzung bei der Auswahl von Empfängern von Push-Benachrichtigungen bereitzustellen.

Bei Verwendung von Java können Sie die Benutzer-ID einer mobilen App wie folgt abrufen.

```
String xid = XtifySDK.getXidKey(getApplicationContext());
```

Die Benutzer-ID einer mobilen App ist erst verfügbar, wenn der mobile Benutzer die App auf einem mobilen Gerät installiert. Wenn Sie die Benutzer-ID der mobilen App an den Server senden möchten, der Ihre Marketing-Datenbank unterstützt, verwenden Sie die XtifyNotifier-Methode `onRegistered`. Suchen Sie in der Beispiel-App im IBM Push Notification SDK nach einem Beispiel dafür, wie die Benutzer-ID einer mobilen App abgerufen werden kann.

Die Benutzer-ID einer mobilen App kann sich in den folgenden Szenarien ändern.

- Ein Gerät wird erneut registriert (erneute Registrierung, wenn bereits eine Benutzer-ID einer mobilen App vorhanden ist). Dies tritt ein, wenn der Benutzer die App erneut installiert. Ein Upgrade der App wirkt sich nicht auf die Benutzer-ID einer mobilen App aus.
- Die Installations-ID ändert sich. Dies ist unwahrscheinlich, könnte jedoch eintreten, wenn es eine technische Änderung am Gerät gibt.

Zugehörige Konzepte:

„Anforderung zur Identifikation von App-Benutzern in der Marketing-Datenbank" auf Seite 91

Integration des Apple Push Notification Service in IBM eMessage

IBM eMessage bietet eine einfache Möglichkeit der Integration des Apple Push Notification Service (APNS) in Ihre Anwendungen für iOS (iPhone & iPad) 3.2 und höher.

Zur Integration von APNS in IBM Messaging-Services müssen Sie das IBM Push-Benachrichtigungs-SDK für Apple iOS herunterladen und integrieren.

Zugehörige Konzepte:

„Voraussetzungen für die Integration von Apple iOS-Apps in IBM Push-Benachrichtigungen" auf Seite 76

Zugehörige Tasks:

„Mobile App in IBM eMessage registrieren" auf Seite 90

Voraussetzungen für die Integration von Apple iOS-Apps in IBM Push-Benachrichtigungen

Bevor Sie mit der Integration einer Apple iOS-App in IBM Services für Push-Benachrichtigungen beginnen, müssen Sie Ihre App für iOS (iPhone & iPad) 3.2 und höher beim Apple Push Notification Service (APNS) registrieren und bereitstellen. Bei der Registrierung konfigurieren Sie ein SSL-Zertifikat und Kennwort. Diese werden für die Verbindung zum APNS benötigt. Das Zertifikat und das Kennwort müssen auch bei der Registrierung der mobilen App bei IBM Messaging-Services eingegeben werden.

Wenn Sie Ihre mobile App bei Apple registrieren und bereitstellen, können Sie ein Entwicklungsprofil und ein Produktionsprofil erstellen. Für jedes Profil wird ein separates SSL-Zertifikat und Kennwort benötigt und die Registrierung beim APNS erfolgt separat. Dieselben Entwicklungs- und Produktionszertifikate und -kennwörter geben Sie separat bei IBM an, wenn Sie die iOS-App bei IBM registrieren.

Die Registrierung und Bereitstellung Ihrer mobilen App bei Apple umfasst die folgenden Schritte:

- Erstellen Sie ein Apple-Entwicklerkonto und laden Sie Xcode herunter.
- Erstellen Sie Ihre App in Xcode.
- Erstellen Sie eine Bundle-ID.
- Erstellen Sie eine explizite App-ID. Erstellen Sie keine Platzhalter-App-ID.
- Registrieren Sie die App beim Apple Push Notification Service. Erstellen Sie Bereitstellungsprofile für Entwicklung und Produktion. Jedes Profil umfasst ein SSL-Zertifikat und ein Kennwort.
- Die App und die App-ID müssen im APNS als für Push-Benachrichtigungen aktiviert angesehen werden.

Beachten Sie unter Apple (https://developer.apple.com/library/mac/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/Chapters/ProvisioningDevelopment.html#//apple_ref/doc/uid/TP40008194-CH104-SW1) die spezifischen Anleitungen zur Registrierung Ihrer mobilen App bei Apple und zur Bereitstellung der App.

Anmerkung: Achten Sie darauf, für jedes Bereitstellungsprofil, das Sie erstellen, den Zertifikatsnamen und das Kennwort aufzuzeichnen. Diese Werte müssen Sie bei der Registrierung der App bei IBM angeben. Vergewissern Sie sich, dass der Zertifikatstyp dem Bereitstellungsprofiltyp entspricht. Für Verteilungsprofile wird ein Verteilungszertifikat benötigt. Für Entwicklungsprofile ist ein Entwicklungsprofil erforderlich.

Zugehörige Konzepte:

„Integration des Apple Push Notification Service in IBM eMessage" auf Seite 75

Zugehörige Tasks:

„Mobile App in IBM eMessage registrieren" auf Seite 90

iOS in Ihrer App implementieren

Wenn Sie iOS-Apps in IBM Messaging-Services integrieren möchten, müssen Sie das IBM Push Notification SDK for Apple iOS herunterladen und Ihrer mobilen App hinzufügen. Ändern Sie das SDK und die mobile App, um die Benachrichtigungsfunktionen bereitzustellen, die IBM eMessage unterstützt.

Vorbereitende Schritte

Bevor Sie Ihre App ändern, um sie zusammen mit eMessage und IBM Messaging-Systemen einzusetzen, sind folgende Maßnahmen zu ergreifen.

- Registrieren Sie Ihre App für den Apple Push Notification Service. Sie müssen das SSL-Zertifikat und das Kennwort speichern. Diese Werte sind für die Implementierung des SDK erforderlich.
- Registrieren Sie die App für eMessage. Im Rahmen des Registrierungsprozesses wird ein App-Schlüssel generiert. Der App-Schlüssel ist für die Implementierung des SDK erforderlich.

Informationen zu diesem Vorgang

Wenn Sie das Push Notification SDK for Apple iOS verwenden möchten, müssen die Quellendateien aus dem SDK-Ordner in das App-Projekt übertragen werden.

Vorgehensweise

1. Laden Sie das Paket IBM Push Notification SDK for Apple iOS von IBM developerWorks unter https://www.ibmdw.net/push/docs/ibm-mobile-push-notification/apple-push-notification-service/download-ibm-push-notification-sdk-apple-ios/ herunter.
2. Öffnen Sie im Apple Provisioning Portal das Projekt **Xcode** für Ihre mobile App.
3. Öffnen Sie das Paket IBM Push Notification SDK for Apple iOS. Ziehen Sie den Ordner XtifyLib aus dem lokalen Ordner (z. B. `/XtifyRich vN.n/XtifyLib`) in das App-Projekt Xcode. Stellen Sie sicher, dass **Copy items into destination group's folder (if needed)** (Einträge in Ordner der Zielgruppe kopieren (falls erforderlich)) ausgewählt ist.
4. Aktualisieren Sie `XtifyGlobal.h`.
   a. Ersetzen Sie xAppKey durch Ihren App-Schlüssel.

   ```
   #define xAppKey @"REPLACE_WITH_YOUR_APP_KEY"
   //Rufen Sie den App-Schlüssel ab, den Sie bei der Registrierung der App
   für den APNS erstellt haben
   ```
5. Fügen Sie Ihrer Projektdatei die folgenden Frameworks hinzu.
   - Foundation.framework
   - UIKit.framework
   - CoreGraphics.framework
   - SystemConfiguration.framework
   - MapKit.framework
   - CoreData.framework
   - MessageUI.framework
   - CoreLocation.framework
   - CFNetwork.framework
   - libxml2.2.dylib
   - libz.1.1.3.dylib
   - MobileCoreServices.framework
   - CoreTelephony.framework
6. In Ihrer AppDelegate-Headerdatei (`AppDelegate.h`):
   a. Fügen Sie `@class XLappMgr;` hinzu.

```
#import <UIKit/UIKit.h>

@class XLappMgr; // Xtify Application Manager – in Ihre App aufnehmen
```

b. Fügen Sie Ihrer App-Implementierungsdatei (`AppDelegate.m`) `#import "XLappMgr.h"` hinzu und nehmen Sie die Elementfunktionen auf, die wie folgt gekennzeichnet sind: **//Nehmen Sie die Funktion in Ihre AppDelegate-Datei auf**.

```
#import "SampleTabsAppDelegate.h"
#import "XLappMgr.h" // Xtify Application Manager – in Ihre App aufnehmen

@implementation SampleTabsAppDelegate

// Nehmen Sie die nachstehenden Funktionen in Ihre AppDelegate-Datei auf
- init
{
 if (self == [super init]) {
  XLXtifyOptions *anXtifyOptions=[XLXtifyOptions getXtifyOptions];
  [[XLappMgr get ]initilizeXoptions:anXtifyOptions];
 }
 return self;
}

// Nehmen Sie diese Funktion in Ihre AppDelegate-Datei auf
- (void)application:(UIApplication *)app
didRegisterForRemoteNotificationsWithDeviceToken:(NSData *)devToken
{
 NSLog(@"Succeeded registering for push notifications. Device token: %@", devToken);
 [[XLappMgr get] registerWithXtify:devToken ];
}

// Nehmen Sie diese Funktion in Ihre AppDelegate-Datei auf
- (void)applicationDidEnterBackground:(UIApplication *)application
{
 NSLog(@"Application is about to Enter Background");
 [[XLappMgr get] appEnterBackground];
}

// Add or incorporate this function in your app delegate file
- (void)applicationDidBecomeActive:(UIApplication *)application {
 NSLog(@"Application moved from inactive to Active state");
 [[XLappMgr get] appEnterActive];
}

// Add or incorporate this function in your app delegate file
- (void)applicationWillEnterForeground:(UIApplication *)application {
 NSLog(@"Application moved to Foreground");
 [[XLappMgr get] appEnterForeground];
}

// Add or incorporate this function in your app delegate file
- (void)application:(UIApplication *)application
didReceiveRemoteNotification:(NSDictionary *)launchOptions
{
   NSLog(@"Receiving notification, app is running");
   NSDictionary * aPush=[[NSDictionary alloc] initWithDictionary:launchOptions];
   [self handleAnyNotification:aPush];
   [aPush release];
}

 // Add or incorporate this function in your app delegate file
- (BOOL)application:(UIApplication *)application
didFinishLaunchingWithOptions:(NSDictionary *)launchOptions
{
  ....Setup main window etc.
    // Überprüfen Sie, ob die App aufgrund einer Push-Benachrichtigung startet
    if ([launchOptions
```

```
   objectForKey:UIApplicationLaunchOptionsRemoteNotificationKey]!=nil)
    {
        NSDictionary * aPush =[launchOptions
      objectForKey:UIApplicationLaunchOptionsRemoteNotificationKey];
        [self handleAnyNotification:aPush];
    }
    return YES;
}

// Nehmen Sie diese Funktion in Ihre AppDelegate-Datei auf
- (void)handleAnyNotification:(NSDictionary *)aPush
{
    // Update Notification Click metrics
    [[XLappMgr get]insertNotificationClick:aPush];
}

// Add or incorporate this function in your app delegate file
-(void)applicationWillTerminate:(UIApplication *)application
{
 NSLog(@"applicationWillTerminate");
 [[XLappMgr get] applicationWillTerminate];
}

- (void)dealloc
{
 [super dealloc];
}

// Nehmen Sie die Funkion in die Anzeige auf, um Simulatorunterstützung zu erhalten
- (void)application:(UIApplication *)application
didFailToRegisterForRemoteNotificationsWithError:(NSError *) error
{
 NSLog(@"Failed to register with error: %@", error);
 [[XLappMgr get] registerWithXtify:nil ];
}

@end
```

7. Wählen Sie im **Xcode-Navigator** Ihr Projekt aus und wählen Sie dann aus der linken Registerkarte **Push Notification** (Push-Benachrichtigung) und aus der rechten Registerkarte **Build Settings** (Buildeinstellungen) aus. Suchen Sie nach **Other Linker Flags** (Sonstige Linker-Flags) und fügen Sie `-ObjC` hinzu.
8. Starten Sie die Kompilierung und dann die Ausführung.

   Die App sollte ordnungsgemäß registriert werden und normal funktionieren. Der Laufzeitfehler `Unrecognized selector` (Auswahl nicht erkannt) bedeutet, dass das Linker-Flag nicht ordnungsgemäß eingerichtet wurde.

Einen App-Eingang für iOS-Apps bereitstellen

Wenn Sie den Versand von Eingangsbenachrichtigungen an eine Apple iOS-App unterstützen möchten, müssen Sie in der mobilen App einen Eingang erstellen, um sie zu empfangen. Eingangsbenachrichtigungen werden auch als erweiterte Benachrichtigungen bezeichnet.

Informationen zu diesem Vorgang

Anmerkung: Weitere Anweisungen im Zusammenhang mit der Implementierung von IBM Push-Benachrichtigungen in Ihrer mobilen App finden Sie in der Beispiel-App, die zusammen mit dem IBM Push Notification SDK for Android bereitgestellt wird.

1. Der XtifyLib-Ordner enthält jetzt Beispielcode zur Erstellung eines angepassten Eingangs. Klassen sind in der Beispielprojektdatei in `XtifyLib` > `CustomInbox` > `AppInclude` enthalten.

2. Verwenden Sie die in AppInclude bereitgestellten Klassen als Ausgangspunkt.
3. Klassen im Überblick:
   a. CompanyCustomInbox – Ein umschließendes Element für Aufrufe für den Abruf von Eingangs-Push-Benachrichtigungen in IBM Mobile Push Notification. Empfangen Sie eine einzige Eingangs-Push-Benachrichtigung und weisen Sie auf anstehende Eingangs-Push-Benachrichtigungen hin. Ändern Sie diese Methoden, wenn Sie ein anderes Verhalten auswählen.
      1) - (void) handleRichPush:(NSString *)msgId;
      2) - (void) getPending:(id)notifyObject;
   b. AppDelegate
      1) Fügen Sie Ihrer ursprünglichen Methode den folgenden Code hinzu:

```
[[CompanyCustomInboxget] setCallbackSelectors:@selector(successfullyGotRichMessage:)
                 failSelector:@selector(failedToGetRichMessage:) andDelegate:self];
```

      2) Implementieren Sie die folgenden Methoden in Ihrem AppDelegate:

```
- (void) successfullyGotRichMessage:(XLRichJsonMessage *)inputMsg // Bei Erfolg benachrichtigen
- (void) failedToGetRichMessage:(CiErrorType )errorType - // Bei Fehler benachrichtigen
```

   c. XRInboxDbInterface – Interne IBM Mobile Push Notification-Klasse zur Bearbeitung der folgenden Funktionen: Zugriff auf IBM Mobile Push Notification-Nutzdaten, ungelesene Nachrichten, Datenspeicher. Nachstehend einige Methoden, die von der Klasse XRInboxDbInterface bereitgestellt werden:
      1) `- (void) updateParentVCandDB:(id)delegatedInboxVC - (void) readLocalStore;`
      2) `- (void) addRichMessageToDb:(XLRichJsonMessage *)inputMsg ;`
      3) `- (int) getUnreadMessageCount;`
      4) `- (int) getMessageCount ;`
      5) `- (int) decrementMessageReadCount ;`
   d. XRInboxUiDbDelegate – Ein Protokoll, das die Benutzerschnittstelle und Datenspeicherereignisse steuert. Verwenden Sie dieses Protokoll, wenn Sie Ihren eigenen View Controller (VC) erstellen, und implementieren Sie die folgenden Methoden:
      1) getInboxDbName – Dateiname für den Datenspeicher.
      2) getInboxEntityName – Entitätsname der Eingangsbenachrichtigung.
      3) getDbModelName – Xcode-Datenmodelldatei. (.xcdatamodel-Erweiterung), die der Datenstruktur der Eingangsbenachrichtigung entspricht.
      4) getInboxTableView – In den meisten Fällen handelt es sich hierbei um den tableView-Eintrag des View Controllers.
      5) didGetPendingResult – Benachrichtigung des Eingangs-VC, wenn der getPending-Aufruf abgeschlossen ist.
   e. CompanyInboxVC – Ansicht der Eingangsbenachrichtigungen – In den meisten Fällen handelt es sich um eine Unterklasse von View Controller und implementiert XRInboxUiDbDelegate (:UITableViewController <XRInboxUiDbDelegate>)
   f. CompanyInboxViewCell – Eine Zellenansicht für jede Zelle. (CompanyInboxViewCell: UITableViewCell)
   g. CompanyDetailsVC – Anzeigeseite der Eingangsbenachrichtigungen (CompanyDetailsVC: UIViewController <UIWebViewDelegate,MFMailComposeViewControllerDelegate>
4. Um die Eingangsliste anzupassen, ändern Sie CompanyInboxVC.xib und CompanyInboxViewCell.xib

5. Um die Ansicht mit Details zu Eingangsbenachrichtigungen anzupassen, ändern Sie CompanyDetailsVC.xib
6. Beispiel:
   a. Instanziieren Sie den angepassten Eingangs-View Controller und aktualisieren Sie die Schnittstelle mit dem View Controller:

```
CompanyInboxVC *inboxVC = [[CompanyInboxVC alloc] initWithNibName:@"CompanyInboxVC" bundle:nil];
Aktualisieren Sie die Datenbankschnittstelle mit der View Controller-Instanz:
[[XRInboxDbInterface get] updateParentVCandDB:inboxVC];
```

   b. Rufen Sie ausstehende Nachrichten ab (z. B. wenn Sie den Navigationscontroller verwenden)

```
NSArray *childViewControllers =inboxNavController.childViewControllers;
 CompanyInboxVC *customVC=childViewControllers[0];
 if (customVC && [customVC respondsToSelector:@selector(getPendingCustom)]) {
           [customVC getPendingCustom];
}
```

   Die getPendingCustom-Methode in Ihrem angepassten View Controller wird informiert, wenn die Serverabfrage abgeschlossen ist. Die Ansicht mit Details zu Eingangsbenachrichtigungen anzeigen, wenn ein Benutzer eine Zeile aus einer Liste auswählt:

```
- (void)tableView:(UITableView *)tableView didSelectRowAtIndexPath:(NSIndexPath *)indexPath
{
  CompanyDetailsVC *detailsViewController=[[CompanyDetailsVC alloc] initWithNibName:@"CompanyDetailsVC"
              bundle:nil];
  RichDbMessage *aDbMessage =  [[XRInboxDbInterface get]  cellForRowAtIndexPath:indexPath];
  [detailsViewController setDetailsFromDbMessage:aDbMessage];
  [self.navigationController pushViewController:detailsViewController animated:YES];
}
```

   c. Bearbeiten Sie die Eingangsbenachrichtigung, wenn die Push-Benachrichtigung empfangen wird, während die App im Vordergrund ausgeführt wird:

```
- (void)application:(UIApplication *)application didReceiveRemoteNotification:(NSDictionary *)pushMessage
{
    NSDictionary * aPush=[[NSDictionary alloc] initWithDictionary:pushMessage];
    [self handleAnyNotification:aPush];
    [aPush release];
}
```

   1) Bearbeiten Sie die Eingangsbenachrichtigung, wenn die App nicht im Vordergrund ausgeführt wird und der Benutzer die native Push-Operation auswählt:

```
- (BOOL)application:(UIApplication *)application didFinishLaunchingWithOptions:
                                                                    (NSDictionary *)launchOptions
{
// Die App startet aufgrund einer Push-Benachrichtigung
if ([launchOptions objectForKey:UIApplicationLaunchOptionsRemoteNotificationKey]!=nil)
    {
NSDictionary * aPush =[launchOptions objectForKey:UIApplicationLaunchOptionsRemoteNotificationKey];
[self handleAnyNotification:aPush];
    }
// Die App startet aufgrund einer wesentlichen Positionsänderung
if ([launchOptions objectForKey:UIApplicationLaunchOptionsLocationKey] != nil )
    {
[[XLappMgr get] handleSignificantLocation:application andOptions:launchOptions];
    }
    return YES;

}
```

   2) Bearbeiten Sie Benachrichtigungen für alle Typen (Eingang, App, angepasst):

```
- (void)handleAnyNotification:(NSDictionary *)aPush
{
    // Aktualisierungsbenachrichtigung zu Klick-Metriken
    [[XLappMgr get]insertNotificationClick:aPush];

    BOOL withAlert=YES;
#if __IPHONE_OS_VERSION_MAX_ALLOWED >= 40000
    // Das Abrufen des Status -applicationState wird erst ab Version 4.0 unterstützt
    if (![[UIApplication sharedApplication] respondsToSelector:@selector(applicationState)])
    {
        withAlert = YES;
    }
    else
    {
        UIApplicationState state = [[UIApplication sharedApplication] applicationState];
        if (state == UIApplicationStateActive) {
            withAlert=YES; // einen Alert anzeigen
        }
        else {
            withAlert =NO; // keinen weiteren Alert anzeigen
        }
    }
#endif

    // Bearbeiten der Eingangsbenachrichtigung unter Verwendung des angepassten Eingangs
    if (aPush !=nil && [aPush objectForKey:@"RN"]!=[NSNull null] &&
                                                    [[aPush objectForKey:@"RN"] length] > 0 )
    {
        [[CompanyCustomInbox get] handleRichPush:aPush withAlert:withAlert];
    }
    // Beenden des angepassten Eingangs

    // Bearbeiten der Open URL-Benachrichtigung
    if (aPush !=nil && [aPush objectForKey:@"URL"] !=[NSNull null] &&
                                                      [[aPush objectForKey:@"URL"] length] > 0 ) {
        NSLog(@"About to Open Safari");
        NSString *urlLink=[[[NSString alloc]initWithString:[aPush objectForKey:@"URL"]]autorelease];
        NSURL *url = [NSURL URLWithString:urlLink];
        if (![[UIApplication sharedApplication] openURL:url]) {
            NSLog(@"Failed to open url:%@",[url description]);
        }
    }

    // Bearbeiten anderer Benachrichtigungen (nachstehend ein Beispiel für eine angepasste
Benachrichtigung zur Anzeige der Maps-App)
    if (aPush !=nil && [aPush objectForKey:@"MAP"] !=[NSNull null] &&
                                                          [[aPush objectForKey:@"MAP"] length] > 0 ) {
        NSString *urlLink=[NSString stringWithFormat:
                                                 @"http://maps.apple.com/?%@",[aPush objectForKey:@"MAP"]];
        NSURL *url = [NSURL URLWithString:urlLink];
        if (![[UIApplication sharedApplication] openURL:url]) {
            NSLog(@"Failed to open Maps:%@",[url description]);
        }
    }
}
```

Aktionen in Benachrichtigungen bereitstellen

Das Senden von Push-Benachrichtigungen über IBM eMessage kann vier mögliche Aktionen umfassen: Open App (App öffnen), Open URL (URL öffnen), Open Inbox (Eingang öffnen) und Custom Action (angepasste Aktion).

In diesem Abschnitt werden die Szenarien definiert, die Sie in Ihrer App einrichten müssen, um einfache Aktionen auszuführen, ferner erfahren Sie, wie Aktionen aus erweiterten Nachrichten ausgeführt werden.

- Open App (App öffnen): Die Standardaktion, wenn ein Benutzer auf Ihre einfache Benachrichtigung zugreift. Hier ist keine Handlung erforderlich.
- Open URL (URL öffnen): Es müssen URLs verarbeitet werden, die an das Gerät gesendet werden, wenn die App im Vorder- und Hintergrund ausgeführt wird. Fügen Sie in Ihrem AppDelegate den folgenden Code hinzu.

```
- (void)application:(UIApplication *)application
    didReceiveRemoteNotification:(NSDictionary *)pushMessage
{
    NSDictionary * aPush=[[NSDictionary alloc] initWithDictionary:pushMessage];

   // Aktualisierungsbenachrichtigung zu Klick-Metriken
    [[XLappMgr get]insertNotificationClick:aPush];

    // Bearbeiten Sie die Open URL-Nachricht
    if (aPush !=nil && [aPush objectForKey:@"URL"] !=[NSNull null] &&
      [[aPush objectForKey:@"URL"] length] > 0 ) {
        NSString *urlLink=[[[NSString alloc]initWithString:
      [aPush objectForKey:@"URL"]]autorelease];
        NSURL *url = [NSURL URLWithString:urlLink];
        if (![[UIApplication sharedApplication] openURL:url]) {
            NSLog(@"Failed to open url:%@",[url description]);
        }
    }

    [aPush release];
}

- (BOOL)application:(UIApplication *)application
   didFinishLaunchingWithOptions:(NSDictionary *)launchOptions
{
   // Überprüfen Sie, ob die App als Ergebnis einer Push-Operation startete
   if ([launchOptions objectForKey:UIApplicationLaunchOptionsRemoteNotificationKey]!=nil) {
       NSDictionary * aPush=[[NSDictionary alloc] initWithDictionary:launchOptions];

       // Aktualisierungsbenachrichtigung zu Klick-Metriken
       [[XLappMgr get]insertNotificationClick:aPush];

       // Bearbeiten Sie die Open URL-Nachricht
       if (aPush !=nil && [aPush objectForKey:@"URL"] !=[NSNull null] &&
      [[aPush objectForKey:@"URL"] length] > 0 ) {
           NSString *urlLink=[[[NSString alloc]initWithString:
         [aPush objectForKey:@"URL"]]autorelease];
           NSURL *url = [NSURL URLWithString:urlLink];
           if (![[UIApplication sharedApplication] openURL:url]) {
               NSLog(@"Failed to open url:%@",[url description]);
           }
       }
   }


 // Die App startet aufgrund einer wesentlichen Positionsänderung
   if ([launchOptions objectForKey:UIApplicationLaunchOptionsLocationKey] != nil ) {
        [[XLappMgr get]handleSignificantLocation:application andOptions:launchOptions ];
   }
   return YES;
}
```

- Open Inbox-Nachricht (Eingang öffnen): Siehe Abschnitt zur Bereitstellung eines App-Eingangs.
- Angepasste Aktionen für einfache Benachrichtigungen: Wenn Sie möchten, dass Ihre App eine angepasste Aktion ausführt (statt dem Öffnen von URLs oder dem Bearbeiten von erweiterten Benachrichtigungen), können Sie eine eigene angepasste Aktion erstellen. Nachdem die App die Benachrichtigung erhalten hat, agiert sie ausgehend vom Wert in den Nutzdaten. Wenn Sie den Wert in den

Nutzdaten dynamisch ändern, agiert die App entsprechend. Zum Beispiel kann die App abhängig vom Nutzdatenwert auf einer anderen Seite in Ihrer App starten oder eine externe App starten und den Nutzdatenwert an die App übertragen.

Das folgende Beispiel veranschaulicht, wie eine angepasste Aktion mit Nutzdaten versendet und in Ihrer App verarbeitet wird. In diesem Beispiel startet die App, nachdem sie die angepasste Benachrichtigung erhält, die Apple Maps-App und bestimmt eine Route von Quelle zu Ziel, wenn diese Informationen über die Nutzdaten weitergegeben werden.

Wählen Sie in der IBM Mobile Push Notification-Konsole in **Button Action** (Schaltflächenaktion) **Custom Data** (Angepasste Daten) aus. Geben Sie in "Custom Data" Quelle und Ziel ein. Beispiel: `{MAP:'daddr=Trenton,+NJ&saddr=NYC'}`. Sie können dies auch von der Push-API aus durchführen.

```
{
    "apiKey":"your_api_key",
    "appKey":"your_app_key",
    "sendAll": false,
    "xids": ["your_xid"],
    "content": {
        "message": "Get direction from your house to the ball game",
        "action": {
            "type": "CUSTOM",
            "data": "{MAP:'daddr=Trenton,+NJ&saddr=NYC'}", "label":"Direction"
         }
   }
 }
```

In Ihrer App in `AppDelegate.m`:

```
- (void)application:(UIApplication *)application didReceiveRemoteNotification:(NSDictionary *)pushMessage
{
    NSDictionary * aPush=[[NSDictionary alloc] initWithDictionary:pushMessage];

   // Aktualisierungsbenachrichtigung zu Klick-Metriken
    [[XLappMgr get]insertNotificationClick:aPush];

    // Angepasste Aktion
    if (aPush !=nil && [aPush objectForKey:@"MAP"] !=[NSNull null] &&
       [[aPush objectForKey:@"MAP"] length] > 0 ) {
        NSString *urlLink=[NSString stringWithFormat:@"http://maps.apple.com/?%@",
       [aPush objectForKey:@"MAP"]];
        NSURL *url = [NSURL URLWithString:urlLink];
        if (![[UIApplication sharedApplication] openURL:url]) {
            NSLog(@"Failed to open Maps app:%@",[url description]);
        }
    }

    [aPush release];
}

- (BOOL)application:(UIApplication *)application
    didFinishLaunchingWithOptions:(NSDictionary *)launchOptions
{
   // Überprüfen Sie, ob die App als Ergebnis einer Push-Operation startete
   if ([launchOptions objectForKey:UIApplicationLaunchOptionsRemoteNotificationKey]!=nil) {
       NSDictionary * aPush=[[NSDictionary alloc] initWithDictionary:launchOptions];
     // Aktualisierungsbenachrichtigung zu Klick-Metriken
      [[XLappMgr get]insertNotificationClick:aPush];


       // Angepasste Aktion
       if (aPush !=nil && [aPush objectForKey:@"MAP"] !=[NSNull null] &&
       [[aPush objectForKey:@"MAP"] length] > 0 ) {
           NSString *urlLink=[NSString stringWithFormat:@"http://maps.apple.com/?%@",
        [aPush objectForKey:@"MAP"]];
```

```
            NSURL *url = [NSURL URLWithString:urlLink];
            if (![[UIApplication sharedApplication] openURL:url]) {
                NSLog(@"Failed to open Maps app:%@",[url description]);
            }
        }
    }

    // Die App startet aufgrund einer wesentlichen Positionsänderung
    if ([launchOptions objectForKey:UIApplicationLaunchOptionsLocationKey] != nil ) {
         [[XLappMgr get]handleSignificantLocation:application andOptions:launchOptions ];
    }

    return YES;
}
```

Nachdem der Benutzer die Benachrichtigung ausgewählt hat, startet die Maps-App und berechnet die Route von New York City nach Trenton im US-Bundesstaat New Jersey.

- Angepasste Aktionen für erweiterte Benachrichtigungen: Die IBM Push Notification-Konsole und das SDK bieten eine Funktion, mit der eine Aktion in die Nachrichtensymbolleiste aufgenommen werden kann. Die Aktion ist auf der Seite mit Details zu Benachrichtigungen als Teil der Symbolleiste verfügbar. Die integrierten verfügbaren Aktionen sind das Öffnen eines Dialers, das Öffnen eines Browsers und angepasste Aktionen. Wenn Sie eine angepasste Aktion an das Gerät senden möchten, erstellen Sie eine Benachrichtigung in der Konsole und definieren Sie eine „primäre Aktion“. In diesem Abschnitt sind die Änderungen beschrieben, die der Entwickler vornehmen muss, damit die angepassten Aktionen ordnungsgemäß funktionieren.

  Informieren Sie in einer Ihrer Klassen den SDK über die Callback-Funktion, mit der die angepasste Aktion bearbeitet werden wird. Sie können in Ihrer AppDelegate-Klasse z. B. eine Methode developerCustomActionMethod definieren und diese Methode benachrichtigen lassen, wenn der Benutzer die angepasste Aktion aus der Benachrichtigungssymbolleiste auswählt. Nachstehend ein Beispiel dafür.

```
...
   [[XLappMgr get] setDeveloperCustomActionSelector:@selector(developerCustomActionMethod:)];
...
```

Implementieren Sie die Aktionsmethode in Ihrer Klasse. Nachstehend ein Implementierungsbeispiel für developerCustomActionMethod:

```
- (void)developerCustomActionMethod:(NSString *)actionData
{
    NSString *address = [actionData stringByAddingPercentEscapesUsingEncoding:NSUTF8StringEncoding];
    NSString *url = [NSString stringWithFormat:@"http://maps.google.com/maps?q=%@", address];

    [[UIApplication sharedApplication] openURL:[NSURL URLWithString:url]];


}
```

Im vorherigen Beispiel öffnet die App, nachdem der Benutzer die Aktion in der Benachrichtigungssymbolleiste ausgewählt hat, die Google Maps-App unter der Adresse, die in den Aktionsdaten bereitgestellt wird. Gleichermaßen können Sie eine angepasste Aktion zur Öffnung anderer iOS-Apps, die in den URL-Schemata von Apple unter definiert sind, oder einer selbsterstellten App definieren.

Positionsgesteuerte Benachrichtigungen für iOS Apps

Die Bereitstellung positionsgesteuerter Benachrichtigungen hängt vom Erhalt von Positionsaktualisierungen ab, die von der App gesendet werden. Standardmäßig verwenden Push-Benachrichtigungen kein GPS für Standortdienste. Stattdessen verwenden Push-Benachrichtigungen die von Apple empfohlene Energiespar-Option zum Abruf von Positionsaktualisierungen.

Wenn die App im Vordergrund ausgeführt wird, fragt der Standortprozess das Betriebssystem nach der aktuellsten Position und überträgt diese an die Standort-API, damit eine Geofence-Analyse durchgeführt werden kann. Während die App im Hintergrund ausgeführt wird, darf die Bibliothek nur den bereitgestellten und von Apple für diese Anwendungsfälle empfohlenen Service für wesentliche Positionsänderungen verwenden. Wenn Sie Ihre App auf Geofence-Push-Operationen testen, werden Sie wahrscheinlich keine positionsgesteuerte Push-Operation erhalten, wenn Ihr Gerät nicht in Bewegung ist. Sie können die App stoppen und erneut starten, um eine Positionsaktualisierung zu erzwingen. Alternativ können Sie eine Position direkt in die Standort-API eingeben, um ein Positionsereignis nachzuahmen.

Wenn in Ihrer App Background Location aktiviert ist, registriert XtifyLib einen Callback, der ausgeführt wird, wenn iOS selbst eine wesentliche Änderung an der Position des Benutzers erkennt (z. B. über einen Mobilfunkmasten, crowdsourced WiFi oder durch Verwendung von GPS durch den Benutzer).

Es besteht eine allgemeine Fehlwahrnehmung in Verbindung mit dem Standortsymbol (purpurrot oder grau) und seiner Beziehung zum GPS-Empfänger. Das Symbol bedeutet nicht unbedingt, dass eine App GPS verwendet hat. Ein purpurrotes Symbol erscheint, wenn eine App kürzlich Ihre Position verwendet hat (dem Benutzer wird auch die Position mitgeteilt unter **Settings > Privacy > Location Services** (Einstellungen > Datenschutz > Standortdienste)). Ein graues Symbol erscheint, wenn eine App in den letzten 24 Stunden Ihre Position verwendet hat. Weitere Informationen über das purpurrote Symbol und Background Location-Optionen sind in diesem Eintrag mit häufig gestellten Fragen enthalten.

Wie bei allen Bedenken hinsichtlich Benutzererkennung ist die Kommunikation entscheidend. Wenn diese Funktionalität verwendet wird, sollten Sie an zwei Orten Produktkopien speichern, aus denen hervorgeht, warum Sie die Position anfordern. Erstens in einem modalen Popup-Fenster, wenn die Anwendung zum ersten Mal installiert wird; zweitens auf der Seite **Application Settings** (Anwendungseinstellungen). Sie sollten auch überlegen, die Verwendung der Position in den Releaseinformationen und in der Beschreibung der App zu erläutern.

Sollte die App einen nützlichen Service bereitstellen, der auf die Positionserkennung zurückzuführen ist, und dieser Nutzen wird dem Benutzer bei der Installation der App beschrieben, nehmen die Benutzer die Standortdienste eher an. Selbst wenn die App die Position nur einmal oder durch einen vom Benutzer initiierten Check-in erhält, wird der Pfeil angezeigt.

Das SDK für positionsgesteuerte Benachrichtigungen konfigurieren

Wenn Sie positionsgesteuerte Nachrichten erstellen möchten, müssen Sie die Standardeinstellungen im IBM Push Notification SDK for Apple iOS ändern.

Informationen zu diesem Vorgang

Navigieren Sie in Xcode zum Ordner `XtifyLib` und bearbeiten Sie die folgenden Optionen.

1. `#define xLocationRequired NO`
   - Wenn Sie diesen Wert auf `YES` setzen, überwachen IBM Messaging-Services wesentliche Positionsänderungen und gleichen sie mit Positionen ab, die Sie in den eMessage-Einstellungen definieren. Der Benutzer der mobilen App

wird mit einer Eingabeaufforderung dazu aufgefordert, Positionserkennung zuzulassen, wenn er die App installiert.

2. `#define xRunAlsoInBackground FALSE`
   - Wird dieser Wert auf `TRUE` gesetzt, überwachen IBM Messaging-Services Positionsänderungen, während die App im Hintergrund ausgeführt wird. Wird der Wert auf `FALSE` gesetzt, überwachen IBM Messaging-Services Positionsänderungen nur, wenn die App im Vordergrund läuft.

Zugehörige Tasks:

„Positionen für die Zustellung nach Positions-Triggering konfigurieren" auf Seite 93

Benutzerdefiniertes Badge-Verhalten konfigurieren

Das Badge-Zählerverhalten wird standardmäßig vom IBM Push Notification SDK for Apple iOS verwaltet. Sie können das Verhalten im SDK aber auch anpassen.

Vorgehensweise

Navigieren Sie in Xcode zum Ordner `XtifyLib` und bearbeiten Sie `XtifyGlobal.h:#define xBadgeManagerMethod XLInboxManagedMethod`.

1. Zur Verwaltung des Badge-Zählers auf dem Client und dem Server auf Basis der ungelesenen Rich-Text-Nachrichten setzen Sie diesen Parameter auf `XLInboxManagedMethod`
2. Zur Verwaltung der Aktualisierung des Badge auf dem Client und dem Server setzen Sie diesen Parameter auf `XLDeveloperManagedMethod`. Dazu müssen Sie in der AppDelegate-Datei Ihre eigene Methode erstellen.

Beispiel

Folgendes Beispiel stammt aus der Beispiel-App aus dem SDK-Paket.

```
// Here's an example on how to handle inbox badge notification changes
- (void) doMyUpdate:(XLappMgr *)appM
{
    NSInteger newBadge=[appM getInboxUnreadMessageCount];
    NSLog(@"The new inbox badge unread message count is=%d",newBadge);
// Set a private count of notifications
    NSInteger privateCounter=0 ;
[appM setSpringBoardBadgeCount:newBadge+privateCounter];
[appM setServerBadgeCount:newBadge];

}
```

Eine Push-Benachrichtigung für die Apple iOS-Beispiel-App erstellen

Das Paket IBM Push Notification SDK for Apple iOS enthält die iOS-Beispiel-App SampleRich.

Vorbereitende Schritte

Bestätigen Sie, dass der Apple Push Notification Service (APNS) für Ihre App-ID aktiviert ist (im Apple Provisioning Portal prüfen). Es ist eine Apple-ID mit Kennwort erforderlich.

Informationen zu diesem Vorgang

Die iOS-Beispiel-App trägt dazu bei, durchgängige Funktionen von IBM Mobile Push Notification, einschließlich App-Push-Benachrichtigungen, Eingangs-Push-Benachrichtigungen und App-Push-Benachrichtigungen, die mit Eingangsbenachrichtigungen kombiniert sind, zu veranschaulichen. Sie können keine Push-Benachrichtigungen auf einem Emulator empfangen. Sie müssen ein Bereitstellungsprofil auf einem Apple-Gerät implementieren.

Vorgehensweise

1. Erstellen Sie einen iPhone-App-Schlüssel in IBM eMessage und laden Sie das APNS-Zertifikat hoch.
2. Öffnen Sie aus dem Menü **Xcode File** (Xcode-Datei) das Projekt SampleRich.
3. Aktualisieren Sie `XtifyGlobal.h` und ersetzen Sie xAppKey durch Ihren App-Schlüssel.
4. Aktualisieren Sie die Datei `SampleRich-Info.plist` und ersetzen Sie die Bundle-ID durch Ihre App-ID (die Sie bei der Registrierung der App im APNS erhalten haben).
5. Aktualisieren Sie die Projektdatei mit Ihrer Bereitstellungsdatei.
6. Erstellen Sie Inhalt im Kommunikationseditor und stellen Sie sicher, dass eine erweiterte Benachrichtigung an Ihre SampleRich-App gesendet wird. Weitere Informationen zum Erstellen von Benachrichtigungen finden Sie im *IBM eMessage-Benutzerhandbuch*.

Alle Benachrichtigungen vom mobilen Gerät löschen

Sie können das SDK ändern, um eine Möglichkeit bereitzustellen, alle von der App auf dem mobilen Gerät empfangenen Benachrichtigungen zu löschen.

Informationen zu diesem Vorgang

Rufen Sie die folgende Methode wie folgt auf:

```
[[XLAppMgr get] removeAllNotifications];
```

App-Registrierungsbenachrichtigung erhalten

Wenn Sie eine Benachrichtigung erhalten wollen, sobald ein mobiler App-Benutzer die App installiert und registriert hat, müssen Sie die Delegierung und Methode festlegen.

Vorgehensweise

Legen Sie die Delegierung und Methode fest, mit der Sie nach Abschluss einer Registrierung benachrichtigt werden wollen.

```
[[XLappMgr get] setInboxDelegate:self]; // The delegate is used to all Xtify delegation methods.
[[XLappMgr get] setDeveloperXidNotificationSelector:@selector(doUpdateDevServer:)];
```

Die Benutzer-ID einer mobilen App (XID) für iOS integrieren

Bei der Benutzer-ID einer mobilen App handelt es sich um eine eindeutige ID, die das System jedem einzelnen Benutzer einer mobilen Anwendung zuweist, wenn dieser Ihre mobile App herunterlädt und installiert. Die Benutzer-ID einer mobilen App wird auch als XID bezeichnet. IBM Messaging-Systeme senden die Benutzer-ID einer mobilen App an das mobile Gerät. Sie müssen Ihre mobile iOS-App konfigurieren, um die ID abzurufen und in der Marketing-Datenbank zur Nutzung bei der Auswahl von Empfängern von Push-Benachrichtigungen bereitzustellen.

Informationen zu diesem Vorgang

Wenn Sie IBM Push-Benachrichtigungen in Ihre App integrieren, müssen Sie die Benutzer-ID der mobilen App in Ihrer Marketing-Datenbank dauerhaft festlegen. Die ID wird zur Adressierung von Push-Benachrichtigungen verwendet.

Sie können die Benutzer-ID einer mobilen App in obj-c wie folgt abrufen.

1. Callback-Methode. Nach der Registrierung für IBM Messaging-Services führt IBM einen Callback Ihrer Wahl mit der zugewiesenen XID aus (ein Beispiel ist in der Beispiel-App enthalten):

```
// geben Sie in XtifyLib unbedingt an, welcher Callback verwendet werden soll, z. B.:

- init
{
    if (self = [super init]) {
...
                [[XLappMgr get] setDeveloperXidNotificationSelector:@selector(doUpdateXid:)];
...
    }
    return self;
}

 - (void) doUpdateXid:(XLappMgr *)appM
{
    NSLog(@"Got XID=%@",[appM getXid]);
}
```

2. Einzelmethode. Führen Sie Folgendes aus, um die XID abzurufen:

```
#import "AppDetailsMgr.h"

...

NSMutableDictionary *appDetailsDict = [[AppDetailsMgr get] getAppDetails];
NSString *xid = [appDetailsDict valueForKey:@"xid"];
```

Die Benutzer-ID einer mobilen App kann sich in den folgenden Szenarien ändern.

- Ein Gerät wird erneut registriert (erneute Registrierung, wenn bereits eine Benutzer-ID einer mobilen App vorhanden ist). Dies tritt ein, wenn der Benutzer die App erneut installiert. Ein Upgrade der App wirkt sich nicht auf die Benutzer-ID einer mobilen App aus.
- Die Installations-ID ändert sich. Dies ist unwahrscheinlich, könnte jedoch eintreten, wenn es eine technische Änderung am Gerät gibt.

Zugehörige Konzepte:

„Anforderung zur Identifikation von App-Benutzern in der Marketing-Datenbank" auf Seite 91

Gehostetes Messaging-Konto für mobiles Messaging aktivieren

Marketiers können über eMessage nur Push-Benachrichtigungen senden, wenn Ihr gehostetes Messaging-Konto für mobiles Messaging aktiviert ist. Um Ihr gehostetes Messaging-Konto für mobiles Messaging zu aktivieren, müssen Sie eine Anfrage an die IBM Email Account Services unter eacctsvc@us.ibm.com richten.

Informationen zu diesem Vorgang

Das Email Account Services-Team sorgt dafür, dass Ihr gehostetes IBM-Messaging-Konto für mobile Push-Benachrichtigungen eingerichtet ist.

Nächste Schritte

Wenn das Email Account Services-Team mit der Einrichtung Ihres Kontos fertig ist, können Sie Ihre mobilen Apps in der eMessage-Konfiguration registrieren.

Mobile App in IBM eMessage registrieren

Damit Marketiers mit eMessage Benachrichtigungen an eine mobile App senden können, müssen Sie die App in eMessage registrieren. Die einzelnen Kombinationen aus mobiler App und mobilem Betriebssystem müssen jeweils separat in der eMessage-Konfiguration registriert werden.

Vorbereitende Schritte

Ob die eMessage-Konfiguration geändert werden kann, hängt von Benutzerrollen und Berechtigungen ab. Überprüfen Sie im Abschnitt über Benutzerrollen und Berechtigungen die Rollen und Berechtigungen, die für Ihre IBM Enterprise Marketing Management (EMM)-Installation konfiguriert sind.

Anmerkung: Damit mobile Apps in eMessage angezeigt und verwaltet werden können, muss Ihrer Benutzerrolle im Bereich der E-Mail-Verwaltung die Berechtigung zum Konfigurieren mobiler Apps zugewiesen sein.

Informationen zu diesem Vorgang

IBM Messaging-Services und eMessage identifizieren eine mobile App anhand einer eindeutigen alphanumerischen Zeichenfolge, dem sogenannten App-Schlüssel. Beim Registrieren einer mobilen App wird ein App-Schlüssel generiert, der die Kombination aus mobiler App und mobilem Betriebssystem angibt. Bei der Registrierung der App wird der App-Schlüssel automatisch der eMessage-Konfiguration hinzugefügt.

Der Zugriff auf die eMessage-Konfiguration erfolgt über das Fenster **eMessage-Einstellungen**.

Vorgehensweise

1. Navigieren Sie zu **Einstellungen** > **eMessage-Einstellungen**.
2. Klicken Sie auf **Liste mit den Schlüsseln mobiler Apps anzeigen**. Das Fenster **Schlüssel mobiler Apps** wird geöffnet.
3. Klicken Sie auf **Schlüssel für mobile Anwendung hinzufügen** .
4. Geben Sie die Informationen zur Kennzeichnung und Beschreibung der App ein.
   - Geben Sie einen Namen für die App ein. Der Marketier wählt beim Konfigurieren einer Push-Benachrichtigung die App anhand des von Ihnen angegebenen Namens aus.
   - Wählen Sie den App-Schlüsseltyp aus.

Sie können **Produktion** oder **Test** auswählen. Der von Ihnen ausgewählte Typ muss mit dem Apple-Bereitstellungsprofil oder dem Google-Projekt übereinstimmen, mit dem die App registriert wurde.

- Wählen Sie eine Standardzeitzone aus.

  Wenn eMessage den Standort des mobilen Empfängergeräts nicht feststellen kann, wird die Standardzeitzone übernommen.

5. Wählen Sie das Betriebssystem aus, unter dem die App ausgeführt wird. Abhängig von dem ausgewählten Betriebssystem werden entsprechende Optionen angezeigt. Geben Sie Werte ein, die beim Registrieren der App bei Apple oder Google definiert wurden.
   - Für **Android** müssen Sie den Google-API-Schlüssel angeben, der für die App konfiguriert ist.
   - Für **iOS** müssen Sie die Zertifikatsdatei für die App auswählen und das Zertifikatskennwort eingeben. Das Zertifikat wird von Apple bereitgestellt.
6. Geben Sie die Sicherheitsrichtlinien an, über die festgelegt wird, welche Marketiers die App in Push-Benachrichtigungskonfigurationen anzeigen und auswählen können. Für die Benutzerrollen der Marketiers, die die App in Push-Konfigurationen auswählen müssen, ist die Berechtigung zum Bearbeiten von Mailings in der Kategorie **Kampagnen** erforderlich.
7. Um die App zur Konfiguration hinzuzufügen, klicken Sie auf **Änderungen speichern**.

Ergebnisse

Das System weist beim Speichern der App-Schlüsselkonfiguration automatisch einen App-Schlüssel zu. Dieser Schlüssel wird als schreibgeschützter Wert im Feld **App-Schlüssel** des Fensters **Schlüssel mobiler Apps** angezeigt.

Zugehörige Konzepte:

„Integration von Google Cloud Messaging in IBM eMessage" auf Seite 64

„Integration des Apple Push Notification Service in IBM eMessage" auf Seite 75

„Voraussetzungen für die Integration von Google Android-Apps in IBM Push-Benachrichtigungen" auf Seite 64

„Voraussetzungen für die Integration von Apple iOS-Apps in IBM Push-Benachrichtigungen" auf Seite 76

„Berechtigungen für Mailings in Campaign" auf Seite 115

Anforderung zur Identifikation von App-Benutzern in der Marketing-Datenbank

Um es Marketiers zu ermöglichen, Push-Benachrichtigungen von mobilen Apps an Zielgruppen zu versenden, müssen lokale Managementprozesse automatisch neue Benutzer-IDs mobiler Apps zu Marketing-Datenbanken hinzufügen, wo Marketiers IBM Campaign verwenden können, um sie auszuwählen. Die Prozesse müssen die Benutzer-IDs der mobilen App automatisch von jedem Mobilgerät abrufen, auf dem die App installiert ist.

Wenn eine Person die mobile App auf einem Mobilgerät installiert, registriert sich das Gerät selbst mit IBM und stellt den App-Schlüssel zur Verfügung, um die App zu identifizieren. IBM-Messaging-Systeme antworten über die Erstellung einer eindeutigen Benutzer-ID für eine mobile App, um die bestimmte Einheit und mobile

App zu identifizieren. IBM-Systeme bestätigen eine erfolgreiche Registrierung durch Übertragung der Benutzer-ID einer mobilen App zum Mobilgerät. Die Benutzer-ID der mobilen App wird auch XID genannt.

Die Benutzer-ID der mobilen App dient als Adresse, an die eMessage Push-Benachrichtigungen sendet. Die ID muss in der lokalen Marketing-Datenbank für die Auswahl durch Marketiers verfügbar sein. Um Push-Benachrichtigungen an ausgewählte Empfänger zu senden, definieren Marketiers ein Personalisierungsfeld in IBM Campaign, das in der Marketing-Datenbank eine Zuordnung zu Benutzer-IDs mobiler Apps herstellt.

Von IBM gehostete Messaging-Systeme können nicht auf die lokalen Tabellen zugreifen, um die neue Benutzer-ID der mobilen App einzufügen. Lokale Systemadministratoren müssen lokale Prozesse, die die ID vom Mobilgerät, auf dem der Wert gespeichert wurde, abrufen können, entwerfen und gestalten. Der Prozess muss auch den Wert in lokalen Marketing-Datenbanken, die IBM Campaign zugeordnet sind, automatisch aufzeichnen können.

Zugehörige Konzepte:

„Die Benutzer-ID einer mobilen App (XID) für Android integrieren" auf Seite 75

Zugehörige Tasks:

„Die Benutzer-ID einer mobilen App (XID) für iOS integrieren" auf Seite 88

Integration der mobilen App auf einem mobilen Gerät testen

Wenn Sie die Integration der mobilen App mit IBM Messaging-Systemen testen möchten, installieren Sie die App auf einem mobilen Gerät, erstellen Sie mit eMessage Push-Benachrichtigung und Sie diese zum Testen an das Gerät senden.

Informationen zu diesem Vorgang

Um die Integration zu testen, müssen Sie Push-Benachrichtigungen senden. Senden Sie die Benachrichtigungen nur an ausgewählte Testempfänger. Weitere Informationen zum Senden von Push-Benachrichtigungen mit IBM eMessage finden Sie im *IBM eMessage-Benutzerhandbuch*.

Vorgehensweise

1. Installieren Sie die mobile App auf einem mobilen Gerät. Durch die Installation der App auf einem mobilen Gerät wird die Kombination aus mobiler App und mobilem Gerät als eindeutiger App-Benutzer bei IBM registriert. Die IBM Messaging-Services erstellen automatisch eine eindeutige Benutzer-ID der mobilen App, eine so genannte XID, und geben diese zurück.
2. Rufen Sie die Benutzer ID der mobilen App vom Testgerät ab. Wenn Sie eine Push-Benachrichtigung für die mobile App konfigurieren, müssen Sie die Benutzer-ID der mobilen App angeben. Mit welcher Methode Sie die Benutzer-ID der mobilen App abrufen, hängt von der Konfiguration der App ab.
3. Konfigurieren Sie eine Push-Operation zum Senden einer Testnachricht an das Testgerät und führen Sie diese aus. Erstellen Sie eine Ausgabelistentabelle (ALT) mit einem Personalisierungsfeld, in dem die Benutzer-ID der mobilen App (XID) als Feldwert wiedergegeben wird. Führen Sie die Push-Operation aus und überprüfen Sie, ob die Benachrichtigung an das mobile Gerät übermittelt wird.

Führen Sie den Test mit einer App-Push-Benachrichtigung oder einer Eingangs-Push-Benachrichtigung aus, je nachdem, welchen Benachrichtigungstyp Sie senden möchten.

Positionen für die Zustellung nach Positions-Triggering konfigurieren

Marketiers können Push-Benachrichtigungen so konfigurieren, dass sie an mobile Geräte gesendet werden, sobald der Benutzer bestimmte Bereiche betritt, also beispielsweise ein Schaufenster anschaut oder eine Werbeveranstaltung besucht. Damit diese Funktionalität unterstützt wird, müssen die Administratoren in der eMessage-Konfiguration die verfügbaren Positionen definieren.

Informationen zu diesem Vorgang

Um eine Position zu definieren, die Marketiers für die Aktivierung der Zustellung nach Positions-Triggering verwenden können, müssen Sie die vollständige physische Adresse angeben. Ebenso müssen Sie einen Radius rund um die Adresse festzulegen, um den Bereich zu definieren, den Empfänger betreten müssen, damit eine Benachrichtigung ausgelöst wird.

Vorgehensweise

1. Navigieren Sie zu **Einstellungen** > **eMessage-Einstellungen**.
2. Klicken Sie auf **Liste mit verfügbaren Positionen anzeigen**. Das Fenster **Positionen** wird geöffnet.
3. Klicken Sie auf **Position hinzufügen** .
4. Geben Sie die vollständige physische Adresse der Position ein, die hinzugefügt werden soll. Klicken Sie auf **Suchen**, um die Position auf einer Karte anzuzeigen.
5. Geben Sie einen Namen für die Position ein.
6. Geben Sie einen Radius ein, um den Bereich rund um die Position zu definieren, in dem eine App-Benachrichtigung ausgelöst wird.

   Vom System wird der Bereich mit einem roten Kreis markiert. Abhängig von dem von Ihnen definierten Radius müssen Sie die Karte erweitern oder reduzieren, um die Auflösung zu erhalten, bei der der hervorgehobene Bereich auf der Karte angezeigt wird.
7. Klicken Sie auf **Änderungen speichern**. Die neue Position wird in der Liste der verfügbaren Positionen angezeigt.

Zugehörige Tasks:

„Positionsgesteuerte Benachrichtigungen für Android-Apps bereitstellen" auf Seite 68

„Das SDK für positionsgesteuerte Benachrichtigungen konfigurieren" auf Seite 86

Positionseigenschaften bearbeiten

Sie können die Einstellungen für einen Standort ändern, der für die standort-getriggerte Zustellung von Push-Benachrichtigungen für mobile Apps zur Verfügung steht.

Vorgehensweise

1. Navigieren Sie zu **Einstellungen** > **eMessage-Einstellungen**.

2. Klicken Sie auf **Liste mit verfügbaren Standorten anzeigen**. Das Fenster **Standorte** wird geöffnet.
3. Suchen Sie den Standort, dessen Eigenschaften Sie bearbeiten möchten, und klicken Sie auf die Liste. Das Fenster **Standorteigenschaften bearbeiten** wird angezeigt.
4. Aktualisieren Sie die Standorteigenschaften.
   - **Ausgewählter Standort**: Geben Sie die vollständige physische Adresse des Standorts ein und klicken Sie auf **Suchen**.
   - **Name**: Geben Sie den Namen ein, der Marketiern angezeigt werden soll, wenn sie diesen Standort zu einem Benachrichtigungs-Push hinzufügen.
   - **Radius**: Geben Sie den Radius um die physische Adresse an, der den Triggerbereich festlegt. Wenn IBM Messaging-Systeme feststellen, dass sich ein mobiles Gerät in den von Ihnen angegebenen Bereich bewegt, sendet das System die für die Push-Benachrichtigung konfigurierte Benachrichtigung an das mobile Gerät. Der Mindestradius beträgt 1000 Meter bzw. die gleiche Entfernung in einer anderen Einheit.
   - **Beschreibung**: Geben Sie eine kurze Beschreibung ein, die Marketiern in der Push-Konfiguration angezeigt wird. Wenn mehrere Standorte definiert sind, hilft diese Beschreibung bei der Unterscheidung der einzelnen Standorte.
5. Speichern Sie die Änderungen.

Verfügbare Positionen für die Zustellung nach Positions-Triggering löschen

Administratoren können Standorte aus der Liste der für die standort-getriggerte Zustellung verfügbaren Standorte löschen.

Vorgehensweise

1. Navigieren Sie zu **Einstellungen** > **eMessage-Einstellungen**.
2. Klicken Sie auf **Liste mit verfügbaren Standorten anzeigen**. Das Fenster **Standorte** wird geöffnet.
3. Wählen Sie die Positionen aus, die gelöscht werden sollen, und klicken Sie auf **Ausgewählte Positionen löschen** .

Standardwerte für mobiles Messaging konfigurieren

Um Push-Benachrichtigungen an eine Liste mit Benutzern von mobilen Apps zu senden, geben Marketiers für jedes Gerät die Benutzer-ID der mobilen App als Wert für ein Personalisierungsfeld an. Das Personalisierungsfeld ist in der Ausgabelistentabelle (Output List Table, OLT) enthalten, in der die Liste der Empfänger von Push-Benachrichtigungen definiert ist. Administratoren können ein Personalisierungsfeld konfigurieren, das standardmäßig zur Angabe der Benutzer-ID der mobilen App ausgewählt wird.

Informationen zu diesem Vorgang

Durch Angabe eines standardmäßigen Personalisierungsfeldes lässt sich der Zeitaufwand der Marketiers für die Konfiguration von Benachrichtigungs-Push-Operationen für mobile Apps reduzieren. Marketiers können jedoch auch ein anderes Personalisierungsfeld zur Angabe des ID-Wertes verwenden.

Vorgehensweise

1. Navigieren Sie zu **Einstellungen** > **eMessage-Einstellungen**.
2. Klicken Sie auf **Standardwerte für mobiles Messaging anzeigen**. Das Fenster **Standardeinstellungen beim mobilen Messaging** wird geöffnet.
3. Geben Sie den Anzeigenamen des Personalisierungsfeldes ein, das die Benutzer-ID der mobilen App für mobile Geräte angibt, die Benachrichtigungen für mobile Apps empfangen.
4. Klicken Sie auf **Änderungen speichern**. Wenn Marketiers eine neue App-Benachrichtigungs-Push-Operation erstellen, wird das neue standardmäßige Personalisierungsfeld angezeigt. Bereits bestehende App-Benachrichtigungs-Push-Konfigurationen bleiben unverändert.

Push-Benachrichtigung-Aufzeichnungsdaten von IBM

Aufzeichnungsdaten für Push-Benachrichtigungen sind nciht standardmäßig verfügbar. Sie müssen anfordern, dass IBM Push-Benachrichtigung-Aufzeichnungsdaten an die lokalen eMessage-Systemtabellen sendet.

Informationen zu diesem Vorgang

Sie müssen Aufzeichnungsdaten für jede Kombination von App und Betriebssystem separat anfordern. Jede Kombination ist einem anderen AppKey zugeordnet. Um beispielsweise Aufzeichnungsdaten für Benachrichtigungen zu empfangen, die an eine mobile App gesendet wurden, die auf iOS und Android ausgeführt wird, müssen sie zwei separate Anforderungen stellen.

IBM-Messaging-Systeme leiten die Antworten über Response and Contact Tracker (RCT) an die eMessage-Systemtabellen weiter.

Vorgehensweise

- Um eine Benachrichtigung über Aufzeichnungsdaten anzufordern, wenden Sie sich über eacctsvc@us.ibm.com an das E-Mail-Konto-Serviceteam.
- Um die Benachrichtigungsantworten zu analysieren, rufen Sie die eMessage-Systemtabellen ab. Weitere Informationen zu den verfügbaren Daten finden Sie im *IBM eMessage System Tables and Data Dictionary*.

Kapitel 8. Dienstprogramme für eMessage

In eMessage stehen eine Reihe von Scripts bereit, mit denen eMessage-Funktionen verwaltet werden.

Sie können die in diesem Abschnitt beschriebenen Dienstprogramme einsetzen, um verschiedene Start- und Administrationsfunktionen durchzuführen. Neben Dienstprogrammen für IBM Marketing Platform verwendet IBM eMessage Dienstprogramme, die sich nur auf eMessage beziehen und die nur zum Verwalten von eMessage-Komponenten verwendet werden.

Weitere Informationen zu sonstigen für Ihre IBM EMM-Installation verfügbaren Dienstprogrammen finden Sie im *IBM Marketing Platform-Administratorhandbuch*.

RLU-Script

Mit dem RLU-Script können Sie den Status des Hochladeprogramms für die Empfängerliste (Recipient List Uploader, RLU) überprüfen.

Anmerkung: Dieses Script kann nicht zum Starten oder Stoppen des RLU verwendet werden. Mit diesem Script können Sie nur den Status der Verbindung zwischen dem RLU und IBM EMM Hosted Services überprüfen.

Das RLU-Script befindet sich in Ihrem Ausgangsverzeichnis von IBM EMM im Verzeichnis `eMessage > bin`. Das eMessage-Verzeichnis ist ein Unterverzeichnis im Campaign-Verzeichnis.

In UNIX- oder Linux-Umgebungen müssen Sie das Script als `rlu.sh` ausführen.

Unter Windows wird das Script über die Eingabeaufforderung als `rlu.bat` ausgeführt.

Syntax

```
rlu -c | --check [-h]
```

Befehle

-c, --check

Prüft, ob RLU ordnungsgemäß konfiguriert und mit IBM EMM Hosted Services verbunden ist.

Optionen

-h, --help

Zeigt die Syntax für das Script an.

Beispiel

So stellen Sie in einer Linux-Umgebung fest, ob RLU mit IBM EMM Hosted Services verbunden ist:

© Copyright IBM Corp. 1999, 2015

```
rlu.sh --check
```

Abhängig vom Status Ihres Systems könnte die Ausgabe dieses Befehls wie das folgende Beispiel aussehen.

```
Configuring Data Source [systemTables]...
Testing configuration for partition partition1
Testing connectivity for partition partition1
Testing user accessibility for partition partition1
Succeeded. List uploader config and connectivity test
succeeded for partition partition1
```

Zugehörige Tasks:

„Upload an IBM EMM Hosted Services testen" auf Seite 41

eMessage-Script für den Response and Contact Tracker (RCT)

Mit diesem Script können Sie den Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) ausführen und seinen Status prüfen.

Dieses Script befindet sich im Verzeichnis `bin` Ihrer eMessage-Installation. Das eMessage-Verzeichnis ist ein Unterverzeichnis im Campaign-Verzeichnis.

In UNIX- oder Linux-Umgebungen müssen Sie das Script als `rct.sh` ausführen.

Unter Windows wird das Script über die Befehlszeile als `rct.bat` ausgeführt.

Syntax

```
rct [ start | stop | check ]
```

Befehle

start

Startet den RCT

stop

Stoppt den RCT

Optionen

check

Prüfen Sie den Status der Verbindung zwischen dem RCT und IBM EMM Hosted Services.

Beispiele

- So starten Sie den RCT unter Windows:

  ```
  rct.bat start
  ```

- So stoppen Sie den RCT unter Windows:

  ```
  rct.bat stop
  ```

- So stellen Sie in einer Linux-Umgebung fest, ob der RCT mit IBM EMM Hosted Services verbunden ist:

```
rct.sh check
```

Abhängig vom Status Ihres Systems könnte die Ausgabe dieses Befehls wie folgt aussehen:

```
C:\<EMM_HOME>\Campaign\eMessage\bin>rct check
Testing config and connectivity for partition partition1
Succeeded | Partition: partition1 - Hosted Services Account ID:
asm_admin
```

Zugehörige Tasks:

„Response and Contact Tracker als Service hinzufügen" auf Seite 37

„Download aus IBM EMM Hosted Services testen" auf Seite 41

eMessage-Script 'MKService_rct'

Mit dem Script 'MKService_rct' kann der Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) als Service hinzugefügt oder entfernt werden. Wenn Sie den RCT als Service hinzufügen, wird er bei jedem Neustart eines Computers, auf dem Sie ihn installiert haben, ebenfalls erneut gestartet. Durch das Entfernen des RCT als Service kann verhindert werden, dass RCT automatisch erneut gestartet wird.

Dieses Script befindet sich im Verzeichnis `bin` Ihrer eMessage-Installation.

In UNIX- oder Linux-Umgebungen muss das Script `MKService_rct.sh.` mit einem Benutzer ausgeführt werden, der über Rootberechtigungen verfügt oder berechtigt ist, Dämonprozesse zu erstellen.

Unter Windows wird das Script über die Befehlszeile als `MKService_rct.bat` ausgeführt.

Syntax

```
MKService_rct -install

MKService_rct -remove
```

Befehle

-install

Fügt den RCT als Service hinzu.

-remove

Entfernt den RCT-Service.

Beispiele

- So fügen Sie den RCT als Windows-Dienst hinzu:
  ```
  MKService_rct.bat -install
  ```
- So entfernen Sie den RCT-Service unter UNIX oder Linux:
  ```
  MKService_rct.sh -remove
  ```

Zugehörige Konzepte:

„Informationen zum automatischen Starten des RCT als Service" auf Seite 36

Zugehörige Tasks:

„Response and Contact Tracker als Service hinzufügen" auf Seite 37

configTool

Die Eigenschaften und Werte auf der Seite **Konfiguration** werden in den Systemtabellen gespeichert. Zum Importieren und Exportieren der Konfigurationseinstellungen aus den Systemtabellen können Sie das Dienstprogramm `configTool` verwenden.

Anwendungsgebiete von "configTool"

Es wird empfohlen, `configTool` für die folgenden Zwecke zu verwenden.

- Zum Importieren der in Campaign bereitgestellten Partitions- und Datenquellenvorlagen, die Sie anschließend auf der Seite **Konfiguration** bearbeiten und duplizieren können.
- Zum Registrieren (Importieren der Konfigurationseigenschaften für) von IBM EMM-Produkten, wenn das Installationsprogramm die Eigenschaften nicht automatisch zur Datenbank hinzufügen kann.
- Zum Exportieren einer XML-Version der Konfigurationseinstellungen zu Sicherungszwecken oder zum Importieren in eine andere Installation von IBM EMM.
- Zum Löschen von Kategorien, die nicht über den Link **Kategorie löschen** verfügen. Exportieren Sie hierfür zunächst Ihre Konfiguration mit `configTool`. Löschen Sie dann manuell die XML, die die Kategorie erstellt, und verwenden Sie `configTool`, um die bearbeitete XML zu importieren.

Wichtig: Dieses Dienstprogramm modifiziert die Tabellen `usm_configuration` und `usm_configuration_values` in der Marketing Platform-Systemtabellendatenbank, die die Konfigurationseigenschaften und die zugehörigen Werte enthalten. Sie sollten entweder Sicherheitskopien dieser Tabellen erstellen oder Ihre aktuellen Konfigurationen mit `configTool` exportieren und die so erstellte Datei sichern. So können Sie Ihre Konfiguration wiederherstellen, falls der Import mit `configTool` fehlschlägt.

Syntax

```
configTool -d -p "Pfad zum Element" [-o]

configTool -i -p "Pfad zum übergeordneten Element" -f Importdatei [-o]

configTool -x -p "Pfad zum Element" -f Exportdatei

configTool -vp -p "Pfad zum Element" -f Importdatei [-d]

configTool -r Produktname -f Registrierungsdatei [-o] configTool -u
Produktname
```

Befehle

-d -p "*Pfad zum Element*" [o]

Löschen der Konfigurationseigenschaften und der entsprechenden Einstellungen durch Angeben eines Pfads in der Hierarchie der Konfigurationseigenschaften.

Im Elementpfad müssen die internen Namen der Kategorien und Eigenschaften verwendet werden. Diese können über die Seite **Konfiguration** abgerufen werden. Wählen Sie hier die gewünschte Kategorie oder Eigenschaft aus. Der entsprechende Pfad wird hierauf auf der rechten Seite des Bildschirms in Klammern angezeigt. Grenzen Sie einen Pfad in der Hierarchie der Konfigurationseigenschaften mit dem Zeichen | ab und setzen Sie den Pfad in doppelte Anführungszeichen.

Beachten Sie Folgendes:

- Mit diesem Befehl können keine ganzen Anwendungen, sondern nur Kategorien und Eigenschaften innerhalb einer Anwendung gelöscht werden. Verwenden Sie den Befehl `-u`, um die Registrierung einer ganzen Anwendung aufzuheben.
- Zum Löschen von Kategorien, für die auf der Seite **Konfiguration** kein Link **Kategorie löschen** angezeigt wird, verwenden Sie die Option `-o`.

Wenn Sie mit dem Befehl `-vp` die Option `-d` verwenden, löscht das Dienstprogramm 'configTool' alle untergeordneten Knoten im angegebenen Pfad, sofern diese Knoten nicht in der angegebenen XML-Datei enthalten sind.

`-i -p "`*`Pfad zum übergeordneten Element`*`" -f `*`Importdatei`*` [o]`

Importieren von Konfigurationseigenschaften und deren Einstellungen aus einer angegebenen XML-Datei.

Zum Importieren geben Sie den Pfad zu dem übergeordneten Element an, unter dem Sie die Kategorien importieren möchten. Das Dienstprogramm `configTool` importiert die Eigenschaften unter der im Pfad angegebenen Kategorie.

Sie können Kategorien auf jeder Ebene unter der obersten Ebene hinzufügen, nicht jedoch auf der Ebene der obersten Kategorie.

Im Pfad zum übergeordneten Element müssen die internen Namen der Kategorien und Eigenschaften verwendet werden. Diese können über die Seite **Konfiguration** abgerufen werden. Wählen Sie hier die erforderliche Kategorie oder Eigenschaft aus. Der entsprechende Pfad wird hierauf auf der rechten Seite des Bildschirms in Klammern angezeigt. Grenzen Sie einen Pfad in der Hierarchie der Konfigurationseigenschaften mit dem Zeichen | ab und setzen Sie den Pfad in doppelte Anführungszeichen.

Sie können für die Importdatei eine Speicherposition mit Bezug auf das Verzeichnis `tools/bin` (relativer Pfad) oder einen vollständigen Verzeichnispfad angeben. Unabhängig davon, ob Sie einen relativen Pfad oder keinen Pfad angeben, sucht `configTool` zunächst nach der Datei mit Bezug auf das Verzeichnis `tools/bin`.

Dieser Befehl überschreibt standardmäßig keine vorhandenen Kategorien, dies kann jedoch über die Option `-o` erzwungen werden.

`-x -p "`*`Pfad zum Element`*`" -f `*`Exportdatei`*

Exportieren von Konfigurationseigenschaften und deren Einstellungen in eine angegebene XML-Datei.

Sie können alle Konfigurationseigenschaften exportieren oder den Export auf eine bestimmte Kategorie beschränken, indem Sie einen Pfad in der Hierarchie der Konfigurationseigenschaften angeben.

Im Elementpfad müssen die internen Namen der Kategorien und Eigenschaften verwendet werden. Diese können über die Seite **Konfiguration** abgerufen werden. Wählen Sie hier die gewünschte Kategorie oder Eigenschaft aus. Der entsprechende Pfad wird hierauf auf der rechten Seite des Bildschirms in Klammern angezeigt. Grenzen Sie einen Pfad in der Hierarchie der Konfigurationseigenschaften mit dem Zeichen | ab und setzen Sie den Pfad in doppelte Anführungszeichen.

Sie können für die Exportdatei eine Speicherposition mit Bezug auf das aktuelle Verzeichnis (relativer Pfad) oder einen vollständigen Verzeichnispfad angeben. Wenn die Dateispezifikation kein Trennzeichen (/ unter UNIX, / oder \ unter Windows) enthält, speichert `configTool` die Datei im Verzeichnis `tools/bin` unter Ihrer Marketing Platform-Installation. Wenn Sie die Dateierweiterung `xml` nicht anfügen, wird diese von `configTool` angefügt.

-vp -p "*Pfad zum Element*" -f *Importdatei* [-d]

Dieser Befehl wird in erster Linie bei manuellen Upgrades zum Import der Konfigurationseigenschaften verwendet. Wenn Sie ein Fixpack mit neuen Konfigurationseigenschaften angewendet haben und danach ein manuelles Upgrade mit dem Import einer Konfigurationsdatei durchführen, kann es passieren, dass Werte, die zuvor durch das Fixpack festgelegt wurden, durch Werte der neuen Konfigurationsdatei überschrieben werden. Mit dem Befehl `-vp` stellen Sie jedoch sicher, dass durch den Import keine zuvor festgelegten Konfigurationswerte geändert werden.

Wichtig: Nach der Ausführung des Dienstprogramms `configTool` mit der Option -vp müssen Sie den Webanwendungsserver, auf dem Marketing Platform implementiert ist, neu starten, damit die Änderungen wirksam werden.

Wenn Sie mit dem Befehl `-vp` die Option `-d` verwenden, löscht das Dienstprogramm 'configTool' alle untergeordneten Knoten im angegebenen Pfad, sofern diese Knoten nicht in der angegebenen XML-Datei enthalten sind.

-r *Produktname* -f *Registrierungsdatei*

Registrieren der Anwendung. Die Speicherposition der Registrierungsdatei kann sich auf das Verzeichnis `tools/bin` beziehen oder ein vollständiger Verzeichnispfad sein. Dieser Befehl überschreibt standardmäßig keine vorhandenen Konfigurationen, dies kann jedoch über die Option `-o` erzwungen werden. Der Parameter *Produktname* muss einer der oben aufgelisteten Namen sein.

Beachten Sie Folgendes:

- Wenn Sie den Befehl `-r` verwenden, muss die XML-Registrierungsdatei als ersten Tag den Tag `<application>` enthalten.

  Möglicherweise werden andere Dateien mit Ihrem Produkt bereitgestellt, mit denen Sie Konfigurationseigenschaften in die Marketing Platform-Datenbank einfügen können. Verwenden Sie für diese Dateien den Befehl `-i`. Nur die Datei, die den Tag `<application>` als ersten Tag enthält, kann mit dem Befehl `-r` verwendet werden.
- Die Registrierungsdatei für die Marketing Platform hat den Namen `Manager_.config.xml` und der erste Tag ist `<Suite>`. Um diese Datei auf einer neuen Installation zu registrieren, verwenden Sie das Dienstprogramm `populateDb`, oder führen Sie das Marketing Platform-Installationsprogramm erneut aus, wie im *IBM Marketing Platform-Installationshandbuch* beschrieben.

- Wenn Sie nach der Erstinstallation andere Produkte als die Marketing Platform erneut registrieren müssen, verwenden Sie `configTool` mit dem Befehl `-r` und `-o`, um die vorhandenen Eigenschaften zu überschreiben.

Das Dienstprogramm `configTool` verwendet Produktnamen als Parameter in den Befehlen für die Produktregistrierung bzw. Aufhebung der Registrierung. In Release 8.5.0 von IBM EMM haben sich viele Produktnamen geändert. Die von `configTool` erkannten Namen haben sich allerdings nicht geändert. Die gültigen Produktnamen für die Nutzung mit `configTool` sowie die aktuellen Namen der Produkte sind nachfolgend aufgeführt.

Tabelle 3. Produktnamen für die Registrierung bzw. Aufhebung der Registrierung mit dem Dienstprogramm "configTool"

Produktname	**In 'configTool' verwendeter Name**
Marketing Platform	`Manager`
Campaign	`Campaign`
Distributed Marketing	`Collaborate`
eMessage	`emessage`
Interact	`interact`
Contact Optimization	`Optimize`
Marketing Operations	`Plan`
CustomerInsight	`Insight`
Digital Analytics for On Premises	`NetInsight`
Opportunity Detect	`Detect`
Leads	`Leads`
Interaction History	`InteractionHistory`
Attribution Modeler	`AttributionModeler`
IBM SPSS Modeler Advantage Enterprise Marketing Management Edition	`SPSS`
Digital Analytics	`Coremetrics`

`-u` *`Produktname`*

Aufheben der Registrierung einer durch *`Produktname`* angegebenen Anwendung. Sie müssen der Produktkategorie keinen Pfad hinzufügen; der Produktname ist ausreichend, jedoch erforderlich. Hierdurch werden alle Eigenschaften und Konfigurationseinstellungen für das Produkt entfernt.

Optionen

`-o`

Überschreibt in Verbindung mit `-i` oder `-r` eine bestehende Kategorie oder Produktregistrierung (Knoten).

Bei Verwendung mit `-d` können Sie eine Kategorie (Knoten) löschen, für die auf der Seite **Konfiguration** kein Link **Kategorie löschen** angezeigt wird.

Beispiele

- Importieren von Konfigurationseinstellungen aus der Datei `Product_config.xml` aus dem Verzeichnis `conf` in der Marketing Platform-Installation.

  ```
  configTool -i -p "Affinium" -f Product_config.xml
  ```

- Importieren einer der bereitgestellten Campaign-Datenquellenvorlagen in die Campaign-Standardpartition "partition1". Das Beispiel setzt voraus, dass Sie die Oracle-Datenquellenvorlage, `OracleTemplate.xml`, im Verzeichnis `tools/bin` unter der Marketing Platform-Installation gespeichert haben.

  ```
  configTool -i -p "Affinium|Campaign|partitions|partition1|dataSources" -f
  OracleTemplate.xml
  ```

- Exportieren aller Konfigurationseinstellungen in die Datei `myConfig.xml` im Verzeichnis `D:\backups`.

  ```
  configTool -x -f D:\backups\myConfig.xml
  ```

- Exportieren einer bestehenden Campaign-Partition (vollständig, mit Datenquelleneinträgen), Speichern in der Datei `partitionTemplate.xml` und Speichern im Standardverzeichnis `tools/bin` unter der Marketing Platform-Installation.

  ```
  configTool -x -p "Affinium|Campaign|partitions|partition1" -f
  partitionTemplate.xml
  ```

- Manuelle Registrierung der Anwendung "Produktname" unter Verwendung der im Standardverzeichnis `tools/bin` in der Marketing Platform-Installation gespeicherten Datei `app_config.xml` und Überschreiben einer bestehenden Registrierung dieser Anwendung.

  ```
  configTool -r Produktname -f app_config.xml -o
  ```

- Aufhebung der Registrierung der Anwendung "Produktname".

  ```
  configTool -u Produktname
  ```

Sichern von Konfigurationseinstellungen

Zur Sicherung der Konfigurationseinstellungen von eMessage und Campaign verwenden Sie das Dienstprogramm `configTool`, um eine Kopie der aktuellen Konfigurationseinstellungen aus IBM Marketing Platform in eine Datei zu kopieren.

Informationen zu diesem Vorgang

Einzelheiten zum Verwenden des Dienstprogramms `configTool`, einschließlich einer Beschreibung der Syntax und der Parameter, finden Sie unter „configTool” auf Seite 100.

Bei der Sicherung mit `configTool` werden alle aktuellen Eigenschaftseinstellungen in der Kategorie `eMessage` in den Konfigurationen exportiert. Geben Sie beim Durchführen der Sicherung einen Dateinamen für die exportierte `.xml`-Datei an und notieren Sie sich die Speicherposition der Datei.

Beispiele

In Windows:

```
configTool.bat -x -p "emessage" -f emessageProperties.xml
```

In UNIX oder Linux:

```
configTool.sh -x -p "emessage" -f emessageProperties.xml
```

Die `.xml`-Datei wird standardmäßig in das Verzeichnis *Manager-Ausgangsverzeichnis*`/xml` exportiert.

Kapitel 9. Informationen zur Fehlersuche bei eMessage

IBM eMessage stellt verschiedene Tools und Verfahren bereit, mit denen Sie Probleme im Zusammenhang mit Ihren Campaign- und eMessage-Installationen untersuchen können.

Protokolldateien für eMessage

IBM EMM stellt mehrere Protokolldateien bereit, die Sie überprüfen können, um Ihre eMessage-Installation zu überwachen und Probleme zu untersuchen.

eMessage-Protokolldatei

Diese Protokolldatei enthält die folgenden Informationsarten, die sich auf von IBM EMM Hosted Services heruntergeladene Informationen beziehen.

- allgemeine Mailing-Informationen
- Mailing-Instanz-ID
- Link-Klick-Daten
- Daten zu unzustellbaren E-Mail-Nachrichten

Die Datei befindet sich im Verzeichnis `logs` unter Ihrer eMessage-Installation.

Temporäre eMessage-Dateien

Diese Dateien enthalten die Daten, die hochgeladen werden.

Die Dateien befinden sich im Verzeichnis `temp` unter Ihrer eMessage-Installation.

Campaign-Protokolldateien

Sie können Protokolldateien in den folgenden Speicherpositionen auf Informationen überprüfen, die sich auf Mailing-Aktivitäten in Campaign beziehen.

- `Campaign\partitions\<partitionN>\logs`

  Verschiedene Protokolldateien, die sich auf Ablaufdiagrammausführungen beziehen, einschließlich Protokolleinträge von im Ablaufdiagramm enthaltenen eMessage-Prozessen.
- `Campaign\logs`

  In diesem Verzeichnis befindet sich die Datei `campaignweb.log`, die Informationen zu Hochladeaktivitäten des Recipient List Uploaders enthält.

Verwenden von log4j mit eMessage

eMessage nutzt das Apache-Dienstprogramm "log4j" zum Protokollieren von Konfigurations-, Debugging- und Fehlerinformationen im Zusammenhang mit dem Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) und dem Hochladeprogramm für die Empfängerliste (RLU).

Informationen zum Ändern der Systemprotokolleinstellungen finden Sie in:

- Den Anmerkungen in der Datei "log4j.properties"

© Copyright IBM Corp. 1999, 2015

- Der Dokumentation zu "log4j" auf der Apache-Website: http://logging.apache.org/log4j/1.2/manual.html

Verwenden von "log4j" mit dem Hochladeprogramm für die Empfängerliste (RLU)

Wenn Sie das Dienstprogramm Recipient List Uploader (RLU) aus der Befehlszeile ausführen, verwendet es Standardeinstellungen für die Protokollfunktion. Um diese Einstellungen zu ändern, müssen Sie die Datei `emsg_rlu_log4j.properties` bearbeiten. Kopieren Sie unter Ihrem eMessage-Installationsverzeichnis im Verzeichnis `conf` die Datei `example_emsg_log4j.properties` nach `emsg_rlu_log4j.properties`. Bearbeiten Sie die Datei `emsg_rlu_log4j.properties` gemäß der Anleitung in den Anmerkungen in dieser Datei.

Wenn das RLU durch ein Ablaufdiagramm automatisch aufgerufen wird, verwendet es die Protokollierung der Campaign-Webanwendung, die in `campaign_log4j.properties` unter Ihrem Campaign-Installationsverzeichnis konfiguriert ist.

Verwenden von "log4j" mit dem Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung)

Wenn Sie das Dienstprogramm Response and Contact Tracker (RCT, Antwort- und Kontaktverfolgung) ausführen, verwendet es Standardeinstellungen für die Protokollfunktion. Um diese Einstellungen zu ändern, müssen Sie die Datei `emsg_rct_log4j.properties` bearbeiten. Kopieren Sie unter Ihrem eMessage-Installationsverzeichnis im Verzeichnis `conf` die Datei `example_emsg_log4j.properties` nach `emsg_rct_log4j.properties`. Bearbeiten Sie die Datei `emsg_rct_log4j.properties` gemäß der Anleitung in den Anmerkungen in dieser Datei.

Kapitel 10. Verwaltung des Benutzerzugriffs auf Messaging-Funktionen

Campaign und eMessage verwenden Rollen und Berechtigungen, die von der IBM Marketing Platform bereitgestellt werden, um den Benutzerzugriff auf Messaging-Funktionen in eMessage und Campaign zu steuern. Um die erforderlichen Änderungen vornehmen zu können, müssen Sie über Berechtigungen in IBM Marketing Platform und Campaign verfügen. Darüber hinaus müssen Sie mit der Konfiguration von Rollen und Berechtigungen in der Marketing Platform sowie mit der Definition von Sicherheitsrichtlinien für Campaign vertraut sein.

E-Mail-Marketer rufen zum Durchführen von E-Mail-Marketing-Kampagnen die eMessage-Mailing-Funktionen in IBM Campaign auf.

Mit den Funktionen und Inhalten im eMessage Document Composer erstellen Marketer personalisierte Kommunikationen und gehostete Landing-Pages.

Allgemeine Informationen zum Konfigurieren von Rollen, Berechtigungen und Richtlinien finden Sie in den entsprechenden Abschnitten im *IBM Marketing Platform-Administratorhandbuch*, in denen die Verwaltung der Sicherheit in IBM Marketing Platform undIBM Campaign beschrieben wird.

Zugehörige Konzepte:

„Rollen- und Richtlinienzuweisung für Mailing-Zugriff"

„Nachrichtenberechtigungen in Campaign" auf Seite 112

„Nachrichtenberechtigungen für eMessage" auf Seite 118

Rollen- und Richtlinienzuweisung für Mailing-Zugriff

Für die Anmeldung beim IBM EMM-System geben E-Mail-Marketer einen Systembenutzernamen und das zugehörige Kennwort ein. Die Berechtigungen, die dem Systembenutzer erteilt wurden, bestimmen, wie der Marketer auf Mailing-Funktionen, personalisierte Kommunikationen und Inhalte in eMessage und Campaign zugreifen kann.

Berechtigungen sind mit Rollen verknüpft, die in der IBM Marketing Platform definiert sind. Sie steuern den Zugriff auf die Mailing-Funktionen in Campaign, indem Sie Rollen in mindestens einer Sicherheitsrichtlinie definieren. Allen Systembenutzern, die auf Mailing-Funktionen, Kommunikationen und Inhalt zugreifen, muss eine eMessage-Rolle in einer Campaign-Sicherheitsrichtlinie zugewiesen sein. Über die Richtlinie wenden Sie selektiv Berechtigungen für Mailing-Funktionen in Campaign sowie für Kommunikationen und Inhalt im eMessage Document Composer an.

Benutzern, die auf Mailing-Funktionen zugreifen, müssen zudem die Benutzer- und Verwaltungsrollen für eMessage zugewiesen werden. Diese Rollen sind von den in den Campaign-Sicherheitsrichtlinien verfügbaren eMessage-Rollen getrennt.

Zugehörige Konzepte:

Kapitel 10, „Verwaltung des Benutzerzugriffs auf Messaging-Funktionen"

„Rollen und Berechtigungen in Marketing Platform und Campaign" auf Seite 110

© Copyright IBM Corp. 1999, 2015

„Nachrichtenberechtigungen in Campaign" auf Seite 112
„Nachrichtenberechtigungen für eMessage" auf Seite 118

Rollen und Berechtigungen in Marketing Platform und Campaign

Rollen in Marketing Platform und Campaign sind eine konfigurierbare Zusammenstellung von Berechtigungen. Sie können für jede Rolle in Marketing Platform und Campaign Berechtigungen angeben, die den Zugriff auf die Anwendung steuern.

Sie können die Standardrollen verwenden oder neue Rollen erstellen. Die verfügbaren Berechtigungen werden vom System definiert. Sie können keine neue Berechtigung erstellen.

Informationen zur Rollenzuweisung

Im Allgemeinen sollten Sie Benutzern Rollen mit Berechtigungen zuweisen, die die Funktionen dieser Benutzer in Ihrem Unternehmen widerspiegeln, wenn sie IBM EMM verwenden. Rollen können einer Gruppe oder einem einzelnen Benutzer zugewiesen werden. Wenn Sie Rollen einer Gruppe zuweisen, hat das folgenden Vorteil: Sie können der Gruppe eine Kombination von Rollen zuweisen und wenn Sie diese Kombination zu einem späteren Zeitpunkt ändern möchten, können Sie dies an einem Ort tun, statt dies mehrfach für mehrere Benutzer durchführen zu müssen. Beim Zuweisen von Rollen zu einer Gruppe nehmen Sie Benutzer in Ihre Gruppen auf oder entfernen Benutzer aus Ihren Gruppen, um den Benutzerzugriff zu steuern.

Bewertung von Rollen durch das System

Wenn ein Benutzer mehrere Rollen hat, bewertet das System die Berechtigungen aus all diesen Rollen zusammen. Die Möglichkeit, eine Funktion für ein bestimmtes Objekt auszuführen, wird ausgehend von den zusammengefassten Berechtigungen aus allen Rollen entweder erteilt oder verweigert. Im Falle von Campaign wird die Möglichkeit, eine Funktion für ein bestimmtes Objekt auszuführen, ausgehend von der Sicherheitsrichtlinie des Objekts erteilt oder verweigert.

Zugehörige Konzepte:

„Rollen- und Richtlinienzuweisung für Mailing-Zugriff" auf Seite 109
„eMessage-Rollen in der globalen Richtlinie" auf Seite 112

Informationen zu Sicherheitsrichtlinien

Sicherheitsrichtlinien sind 'Regelbücher' für die Sicherheit in IBM Campaign. Sie werden immer zu Rate gezogen, wenn ein Benutzer eine Aktion in der Anwendung ausführt. Sicherheitsrichtlinien werden pro Partition erstellt. Sie können nicht partitionsübergreifend gemeinsam genutzt werden. Jede Partition in IBM Campaign kann über mehrere Sicherheitsrichtlinien verfügen.

Eine Sicherheitsrichtlinie besteht aus mehreren von Ihnen definierten Rollen. Jede Rolle enthält eine Gruppe von Berechtigungen, die festlegen, welche Aktionen Benutzer ausführen und auf welche Objekte sie zugreifen können. Sie können entweder einzelne Benutzer direkt oder aber Gruppen zu einer Rolle zuordnen (dabei wird die Rolle den Benutzern in den betreffenden Gruppen zugewiesen).

Wenn Sie ein Objekt wie z. B. eine Kampagne oder ein Angebot im Ordner der höchsten Ebene erstellen, wenden Sie eine Sicherheitsrichtlinie auf das Objekt an. Beim Erstellen eines Ordners der höchsten Ebene wird außerdem eine Sicherheitsrichtlinie auf den Ordner angewendet. Alle Objekte oder Unterordner, die Sie in diesem Ordner erstellen, übernehmen die Sicherheitsrichtlinie des Ordners.

Wenn Sie Sicherheitsrichtlinien auf Objekte oder Ordner anwenden, können Sie die Objekte in IBM Campaign für die Verwendung durch verschiedene Benutzergruppen aufteilen. Sie könnten z. B. Ihre Sicherheitsrichtlinien so konfigurieren, dass die Benutzer, die einer Richtlinie zugehören, nicht auf Objekte zugreifen bzw. Objekte nicht einmal anzeigen können, die anderen Richtlinien zugeordnet sind.

Sie können eigene Sicherheitsrichtlinien erstellen oder die globale Standardsicherheitsrichtlinie verwenden, die in IBM Campaign verfügbar ist.

Globale Sicherheitsrichtlinie

Campaign beinhaltet eine globale Standardsicherheitsrichtlinie, die Sie unverändert verwenden oder den Anforderungen Ihres Unternehmens entsprechend ändern können. Wenn Sie keine eigenen Sicherheitsrichtlinien erstellen möchten, wird die globale Sicherheitsrichtlinie standardmäßig auf die Objekte angewendet, die Sie in Campaign erstellen.

Sie können die globale Richtlinie zusätzlich zu Ihren eigenen Richtlinien verwenden oder ausschließlich eigene Richtlinien anwenden. Die globale Richtlinie kann nicht gelöscht werden, selbst wenn sie nicht verwendet wird.

Alle Sicherheitsrichtlinien, die Sie erstellen, bestehen unter der globalen Sicherheitsrichtlinie. Unter der globalen Richtlinie könnten Sie separate Sicherheitsrichtlinien für die Mitarbeiter der einzelnen Abteilungen in Ihrer Organisation erstellen.

Die globale Sicherheitsrichtlinie enthält sechs vordefinierte Rollen. Bei Bedarf können der globalen Richtlinie weitere Rollen hinzugefügt werden. Sie können die vordefinierten Rollen nicht löschen, jedoch die zugehörigen Berechtigungen ändern.

Die vordefinierten Rollen lauten wie folgt:

- **Folder Owner** (Ordnerbesitzer) - Alle Berechtigungen sind aktiviert.
- **Owner** (Besitzer) - Alle Berechtigungen sind aktiviert.
- **Administrator** - Alle Berechtigungen sind aktiviert. Diese Rolle ist dem Standardbenutzer `asm_admin` zugewiesen.
- **Execute** (Ausführen) - Alle Berechtigungen sind aktiviert.
- **Design** - Es besteht Lese- und Schreibberechtigung für die meisten Objekte. Es ist nicht möglich, Ablaufdiagramme oder Sitzungen zu planen.
- **Review** (Prüfung) - Nur Leseberechtigung

Die globale Sicherheitsrichtlinie gilt für alle Benutzer bis zu den Rollen 'Owner' (Besitzer) und 'Folder Owner' (Ordnerbesitzer), einschließlich der Benutzer, denen keine andere spezifische Rolle in der globalen Richtlinie zugewiesen wurde. Da die globale Richtlinie immer angewendet wird, können damit z. B. auch global Berechtigungen für eine Rolle verweigert werden.

Zugehörige Konzepte:

„eMessage-Rollen in der globalen Richtlinie" auf Seite 112

eMessage-Rollen in der globalen Richtlinie

Neben den vordefinierten Campaign-Rollen enthält die globale Richtlinie mehrere Rollen, die eigens für eMessage vorgesehen sind.

Die globale Richtlinie enthält die folgenden eMessage-Rollen.

- **eMsg_admin** - Darf auf alle Mailing-Funktionen, den gesamten Inhalt und alle Dokumente zugreifen.
- **eMsg_execute** - Darf auf alle Mailing-Funktionen, den gesamten Inhalt und alle Dokumente zugreifen.
- **eMsg_design** - Darf auf den gesamten Inhalt, alle Dokumente und die meisten Mailing-Funktionen zugreifen. Ihr wurde jedoch explizit keine Berechtigung zum Senden von Produktionsmailings erteilt.
- **eMsg_review** - Darf Inhalt und Dokumente nur anzeigen und hat eingeschränkte Berechtigungen zum Arbeiten mit Mailings. Ihr wurde explizit keine Berechtigung zum Hinzufügen, Bearbeiten oder Löschen von Mailings erteilt. Sie darf jedoch Test- und Produktionsmailings anzeigen und senden.

Anmerkung: eMessage unterstützt die standardmäßig für Campaign erstellten Rollen 'Besitzer' und 'Ordnerbesitzer' nicht.

Zugehörige Konzepte:

„Rollen und Berechtigungen in Marketing Platform und Campaign" auf Seite 110

„Globale Sicherheitsrichtlinie" auf Seite 111

„Berechtigungen für Mailings in Campaign" auf Seite 115

„Berechtigungen für die Kategorie 'Digitale Assets'" auf Seite 116

„Berechtigungen für die Kategorie 'Dokumente'" auf Seite 117

Nachrichtenberechtigungen in Campaign

Campaign steuert den Benutzerzugriff auf Mailing-Funktionen durch Aktivieren oder Inaktivieren bestimmter Berechtigungen, die in Rollen definiert sind, welche einem Benutzer oder einer Gruppe zugewiesen sind. Diese Rollen sind einer oder mehreren Sicherheitsrichtlinien zugeordnet. Sie können mehrere Campaign-Sicherheitsrichtlinien definieren und jeder Richtlinie mehrere Rollen zuweisen. Jede Kombination aus Richtlinie und Rollen kann eine bestimmte Berechtigungsgruppe definieren.

Weitere Informationen zum Verwalten von Sicherheitsberechtigungen sowie Beispielszenarios zur Sicherheit finden Sie im *IBM Campaign-Administratorhandbuch*.

Unter 'Rollen und Berechtigungen für die IBM Marketing Platform' weisen Sie, wie nachfolgend beschrieben, Benutzerberechtigungen für Mailing-Funktionen und Inhalt im Campaign-Bereich zu.

1. Definieren Sie Benutzerrollen.

   Systemdefinierte Benutzerrollen für eMessage werden standardmäßig unter der globalen Richtlinie erstellt.

   Sie können auch angepasste Rollen definieren und sie der globalen Richtlinie oder anderen Richtlinien hinzufügen, die Sie definiert haben.
2. Definieren Sie Sicherheitsrichtlinien und fügen Sie den Richtlinien Benutzerrollen hinzu.

Die globale Richtlinie ist standardmäßig definiert. Sie können weitere Richtlinien für Campaign definieren.

3. Definieren Sie bestimmte Berechtigungen für jede Rolle in jeder Richtlinie.

   Sie können zusätzliche Richtlinien und angepasste Rollen mit unterschiedlichen Berechtigungen definieren, um mehr Kontrolle über den Zugriff auf Mailing-Funktionen in Campaign und den eMessage Document Composer zu haben.

Änderungen an Berechtigungen, Rollen und Richtlinien treten bei Anmeldung des Benutzers bei IBM EMM in Kraft. Nachdem Sie einem Benutzer Mailing-Berechtigungen zugewiesen oder seine Mailing-Berechtigungen geändert haben, muss sich der Benutzer abmelden und anschließend wieder anmelden, damit die Änderungen erkannt werden.

Zugehörige Konzepte:

Kapitel 10, „Verwaltung des Benutzerzugriffs auf Messaging-Funktionen", auf Seite 109

„Rollen- und Richtlinienzuweisung für Mailing-Zugriff" auf Seite 109

Rollen und Berechtigungen zur Verfügung stellen

Abhängig von Ihrer IBM Marketing Platform-Installation sind die zum Definieren und Anwenden von Rollen und Berechtigungen erforderlichen administrativen Steuerelemente unter Umständen nicht sofort sichtbar. Sie können die erforderlichen Steuerelemente sichtbar machen, indem Sie den eMessage Document Composer oder ein Mailing in Campaign aufrufen.

Informationen zu diesem Vorgang

Gehen Sie wie nachfolgend beschrieben vor, wenn Sie nicht alle der folgenden Berechtigungen unter der globalen Campaign-Richtlinie sehen.

- Berechtigungen für Mailings in der Kategorie 'Kampagnen'
- Berechtigungen für die Inhaltsbibliothek in der Kategorie 'Digitale Assets'
- Berechtigungen für eMessage-Dokumente in der Kategorie 'Dokumente'

Vorgehensweise

1. Melden Sie sich bei IBM EMM an.

   Wenn Sie mehrere Benutzer konfiguriert haben, melden Sie sich als Benutzer mit den minimalsten Berechtigungen an. Melden Sie sich beispielsweise als Benutzer an, der nur über eine Anzeigeberechtigung verfügt.

2. Navigieren Sie zu **Campaign** > **eMessage Documents** (Campaign > eMessage-Dokumente), um den Document Composer aufzurufen.

   Warten Sie, bis der Document Composer vollständig geladen wurde.

3. Navigieren Sie zu **Settings** > **User Roles and Permissions** > **Campaign** > **partition [n]** > **Global Policy** (Einstellungen > Benutzerrollen und Berechtigungen > Campaign > Partition [n] > Globale Richtlinie).

   Bestätigen Sie in der Eingabeaufforderung, dass Sie den Document Composer verlassen möchten, indem Sie die Seite verlassen.

4. Klicken Sie auf **Add Roles and Assign Permissions** (Rollen hinzufügen und Berechtigungen zuweisen). Die folgenden eMessage-Rollen sind sichtbar.
   - eMsg_admin
   - eMsg_execute

- eMsg_design
- eMsg_review

5. Klicken Sie auf **Save and Edit Permissions** (Berechtigungen speichern und bearbeiten).

   Mailing-Berechtigungen sind in den Kategorien 'Kampagnen', 'Digitale Ressourcen' und 'Dokumente' sichtbar.

   Weitere Informationen zu bestimmten verfügbaren Berechtigungen finden Sie in den folgenden Abschnitten.

Zugehörige Konzepte:

„Berechtigungen für Mailings in Campaign" auf Seite 115

„Berechtigungen für die Kategorie 'Digitale Assets'" auf Seite 116

„Berechtigungen für die Kategorie 'Dokumente'" auf Seite 117

Evaluierung von Berechtigungen in Campaign

Wenn ein Benutzer eine Task ausführt oder versucht, auf ein Objekt zuzugreifen, werden in Campaign folgende Schritte ausgeführt:

1. Es werden alle Gruppen und Rollen bestimmt, denen der Benutzer innerhalb der globalen Sicherheitsrichtlinie angehört. Ein Benutzer kann einer, mehreren oder keiner Rolle zugehören. Benutzer gehören der Rolle 'Owner' (Besitzer) an, wenn sie ein Objekt besitzen; sie gehören der Rolle 'Folder Owner' (Ordnerbesitzer) an, wenn sie Besitzer des Ordners sind, in dem sich ein Objekt befindet. Ein Benutzer gehört nur dann einer anderen Rolle an, wenn er dieser Rolle speziell zugewiesen wurde (entweder direkt oder aufgrund der Zugehörigkeit zu einer Gruppe, die der betreffenden Rolle zugewiesen ist).
2. Es wird bestimmt, ob das Objekt, auf das zugegriffen wird, einer benutzerdefinierten Richtlinie zugeordnet wurde, falls eine solche vorhanden ist. Ist dies der Fall, werden vom System alle Gruppen und Rollen bestimmt, denen der Benutzer innerhalb dieser benutzerdefinierten Richtlinie angehört.
3. Die Berechtigungen für alle Rollen, denen der Benutzer angehört, werden zusammengefasst, basierend auf Ergebnissen der Schritte 1 und 2. Anhand der zusammengefassten Rolle prüft das System die Berechtigungen für die Aktion wie folgt:
   a. Wenn Rollen für diese Aktion die Berechtigung **Abgelehnt** zugewiesen ist, darf der Benutzer diese Aktion nicht durchführen.
   b. Wenn keiner Rolle für diese Aktion die Berechtigung **Abgelehnt** zugewiesen ist, wird überprüft, ob einer Rolle für diese Aktion die Berechtigung **Gewährt** zugewiesen wurde. Falls ja, kann der Benutzer die Aktion ausführen.
   c. Wenn weder A noch B zutreffen, wird dem Benutzer die Berechtigung verweigert.

Definition der Berechtigungsstatus

Sie können für jede Rolle angeben, welche Berechtigungen erteilt, nicht erteilt oder verweigert werden. Sie legen diese Berechtigungen auf der Seite **Settings > User Roles & Permissions** (Einstellungen > Benutzerrollen und Berechtigungen) fest.

Diese Status haben folgende Bedeutungen.

- **Granted** (Erteilt) - wird durch ein grünes Hakensymbol angezeigt. Erteilt ausdrücklich die Berechtigung, diese bestimmte Funktion auszuführen, sofern keine der anderen Rollen des Benutzers die Berechtigung nicht ausdrücklich untersagt.

- **Denied** (Verweigert) - wird durch ein rotes "X" angezeigt. Untersagt ausdrücklich die Berechtigung, diese bestimmte Funktion auszuführen – ungeachtet eventueller Berechtigungserteilungen durch andere Rollen des Benutzers.

- **Not Granted** (Nicht erteilt) - wird durch ein schattiertes graues "X" angezeigt. Die Berechtigung zur Ausführung einer bestimmten Funktion wird weder explizit erteilt noch explizit verweigert. Falls diese Berechtigung nicht ausdrücklich durch eine andere Rolle des Benutzers erteilt wird, ist der Benutzer nicht berechtigt, diese bestimmte Funktion auszuführen.

Berechtigungen für Mailings in Campaign

In Campaign können Sie eMessage-Mailings über Steuerelemente auf den eMessage-Mailing-Registerkarten erstellen, konfigurieren, ausführen und überwachen. Jedes Mailing wird auf einer eigenen Registerkarte verwaltet.

Die folgenden Berechtigungen steuern den Benutzerzugriff auf die eMessage-Mailing-Registerkarten. Sie befinden sich in der Kategorie **Kampagnen**.

Berechtigung	Beschreibung
View Mailings (Mailings anzeigen)	Ermöglicht einem Benutzer die Anzeige einer eMessage-Mailing-Registerkarte in einer Kampagne. Der Benutzer kann das Mailing weder bearbeiten noch ändern.
Edit Mailings (Mailings bearbeiten)	Ermöglicht einem Benutzer die Konfiguration oder Änderung einer eMessage-Mailing-Registerkarte in einer Kampagne.
Delete Mailings (Mailings löschen)	Ermöglicht einem Benutzer das Entfernen eines eMessage-Mailings aus einer Kampagne.
Add Mailings (Mailings hinzufügen)	Ermöglicht einem Benutzer die Erstellung eines Mailings in einer Kampagne.
Send production mailing (Produktionsmailing senden)	Ermöglicht einem Benutzer die Einleitung einer Produktionsausführung des Mailings, die Aktivierung eines Mailings für Transaktions-E-Mails oder die Planung einer Produktionsausführung für ein Mailing. Produktionsmailings können viele Nachrichten enthalten. E-Mail-Nachrichten werden an jede Einzelperson gesendet, die in der Empfängerliste für das jeweilige Mailing als Produktionsempfänger angegeben ist.
Execute test run (Testlauf ausführen)	Ermöglicht einem Benutzer die Einleitung eines Testlaufs des Mailings. Testmailings enthalten für gewöhnlich nur wenige Nachrichten. Während eines Testlaufs wird eine E-Mail-Nachricht an jede Adresse gesendet, die in der Empfängerliste für das jeweilige Mailing als Testempfänger angegeben ist.

Zugehörige Konzepte:

„eMessage-Rollen in der globalen Richtlinie" auf Seite 112

Zugehörige Tasks:

„Mobile App in IBM eMessage registrieren” auf Seite 90
„Rollen und Berechtigungen zur Verfügung stellen” auf Seite 113

Berechtigungen für die Kategorie 'Digitale Assets'

Die Berechtigungen für 'Digitale Assets' steuern den Benutzerzugriff auf Inhaltselemente in der eMessage-Inhaltsbibliothek sowie auf Ordner und Unterordner, in denen die Inhaltselemente gespeichert sind.

Die Inhaltsbibliothek ist ein Repository für Inhaltselemente (auch 'digitale Assets' genannt), die in Kommunikationen verwendet werden, die Benutzer im eMessage Document Composer erstellen.

Berechtigungen	Beschreibung
View eMessage digital assets (Digitale eMessage-Assets anzeigen)	Ermöglicht es einem Benutzer, Inhaltselemente zu öffnen, um Eigenschaften anzuzeigen und eine Vorschau der Inhalte, die einer personalisierten Kommunikation hinzugefügt werden können, zu sehen.
Create new digital assets in the eMessage content library (Neue digitale Assets in der eMessage-Inhaltsbibliothek erstellen)	Ermöglicht es einem Benutzer, ein Inhaltselement zu erstellen und der Inhaltsbibliothek hinzuzufügen.
Edit existing digital assets in the eMessage content library (Bestehende digitale Assets in der eMessage-Inhaltsbibliothek bearbeiten)	Ermöglicht es einem Benutzer, bestehende Inhaltselemente zu öffnen und zu bearbeiten.
Delete digital assets from the eMessage content library (Digitale Assets aus der eMessage-Inhaltsbibliothek löschen)	Ermöglicht es einem Benutzer, ein Inhaltselement aus der Inhaltsbibliothek zu entfernen.
Move digital assets from one folder to another (Digitale Assets aus einem Ordner in einen anderen verschieben)	Ermöglicht es einem Benutzer, Inhaltselemente innerhalb der Inhaltsbibliothek zu verschieben. Damit ein Inhaltselement verschoben werden kann, muss diese Berechtigung den Quellen- und Zielordnern zugewiesen sein.

Zugehörige Konzepte:

„eMessage-Rollen in der globalen Richtlinie” auf Seite 112

Zugehörige Tasks:

„Rollen und Berechtigungen zur Verfügung stellen” auf Seite 113

Berechtigungen für die Kategorie 'Dokumente'

Die Berechtigungen in der Kategorie **Dokumente** steuern den Benutzerzugriff für die Erstellung, Bearbeitung und Verwaltung personalisierter Kommunikationen im eMessage Document Composer.

Berechtigung	Beschreibung
eMessage-Dokumente anzeigen	Ermöglicht einem Benutzer die Anzeige eines Dokuments, das zum Erstellen einer E-Mail, einer Inbox-Push-Benachrichtigung oder einer Landing-Page verwendet wird.
Neue eMessage-Dokumente erstellen	Ermöglicht es einem Benutzer, eine neue personalisierte Kommunikation zu erstellen.
Bestehende eMessage-Dokumente bearbeiten	Ermöglicht es einem Benutzer, eine bestehende personalisierte Kommunikation zu ändern.
eMessage-Dokumente löschen	Ermöglicht es einem Benutzer, eine personalisierte Kommunikation zu entfernen.
eMessage-Dokument veröffentlichen, um Inhalte im öffentlichen Internet verfügbar zu machen	Ermöglicht es einem Benutzer, eine personalisierte Kommunikation zu veröffentlichen. Durch die Veröffentlichung einer Kommunikation werden das Dokument und alle hinzugefügten Inhalte für die Verwendung in einem eMessage-Mailing verfügbar.
eMessage-Dokumente aus einem Ordner in einen anderen kopieren	Ermöglicht es einem Benutzer, eine personalisierte Kommunikation zwischen Ordnern in der Inhaltsbibliothek zu kopieren. Für das Kopieren einer Kommunikation ist diese Berechtigung für den Quell- und den Zielordner erforderlich.
eMessage-Dokumente aus einem Ordner in einen anderen verschieben	Ermöglicht es einem Benutzer, eine personalisierte Kommunikation aus einem Ordner in einen anderen in der Inhaltsbibliothek zu verschieben. Für das Verschieben einer Kommunikation ist diese Berechtigung für den Quell- und den Zielordner erforderlich.

Zugehörige Konzepte:

„eMessage-Rollen in der globalen Richtlinie" auf Seite 112

Zugehörige Tasks:

„Rollen und Berechtigungen zur Verfügung stellen" auf Seite 113

Berechtigungen für die Kategorie 'E-Mail-Verwaltung'

Die Berechtigungen in der Kategorie 'E-Mail-Verwaltung' der globalen Richtlinie von Campaign stellen eMessage-Administratoren den Zugriff auf Einstellungen zur Verfügung, mit denen sie den Benutzerzugriff auf verschiedene Messaging-Domänen und Messaging-Funktionen steuern können.

Administratoren weisen den Zugriff auf Domänen und Funktionen in dem Abschnitt für Richtlinieneinstellungen des Fensters mit den eMessage-Einstellungen zu. Der Administrator kann beispielsweise die Liste der E-Mail-Domänen beschränken, die ein Benutzer als Absenderdomäne (**Von:**) in einer E-Mail-Kommunikation auswählen kann, welche im Kommunikationseditor erstellt wird. Der Abschnitt mit den Richtlinieneinstellungen wird nur dann angezeigt, wenn dem Administrator in der globalen Richtlinie von Campaign explizit eine entsprechende Berechtigung erteilt wurde.

Administratoren können außerdem den Zugriff auf die Verwaltungsschnittstellen für die Registrierung von mobilen Apps bei eMessage steuern. Zudem können sie den Zugriff auf die Verwaltungsschnittstellen für die Konfiguration von Positionen steuern, die beim positionsabhängigen Auslösen der Zustellung verwendet werden. Die Links zu den Verwaltungsseiten werden im Abschnitt mit den Einstellungen für mobile Benachrichtigungen auf der Seite der eMessage-Einstellungen angezeigt. Das mobile Messaging muss für das gehostete Messaging-Konto aktiviert sein, damit der Abschnitt mit den Einstellungen für mobile Benachrichtigungen auf der Seite der eMessage-Einstellungen angezeigt wird.

Berechtigung	Beschreibung
Configure Domains (Domänen konfigurieren)	Steuert den Zugriff auf den Abschnitt für Richtlinieneinstellungen auf der Seite mit den eMessage-Einstellungen. Wenn der Administratorrolle keine Berechtigung für das Konfigurieren von E-Mail-Domänen erteilt wurde, kann der Administrator den Abschnitt für Richtlinieneinstellungen nicht sehen. Diese Berechtigung ist auch für die Verwaltung von Kurzlinkdomänen erforderlich.
Configure Mobile Apps (Mobile Apps konfigurieren) (Nur verfügbar, wenn mindestens das Fixpack Campaign 9.1.0.2 installiert wurde.)	Steuert den Zugriff auf das Fenster **Mobile App Keys** (Schlüssel mobiler Apps) in den eMessage-Einstellungen. Wenn der Administratorrolle keine Berechtigung für das Konfigurieren von mobilen Apps erteilt wurde, wird der Link zu der Seite **Mobile App Keys** (Schlüssel mobiler Apps) nicht auf der Seite mit den eMessage-Einstellungen angezeigt.
Configure Locations (Positionen konfigurieren) (Nur verfügbar, wenn mindestens das Fixpack Campaign 9.1.0.2 installiert wurde.)	Steuert den Zugriff auf das Fenster **Locations** (Positionen) in den eMessage-Einstellungen. Wenn der Administratorrolle keine Berechtigung für das Konfigurieren von Positionen erteilt wurde, wird der Link zu der Seite **Locations** (Positionen) nicht auf der Seite mit den eMessage-Einstellungen angezeigt.

Nachrichtenberechtigungen für eMessage

IBM eMessage steuert den Zugriff auf Mailing-Funktionen außerhalb der Mailing-Registerkarte in Campaign über die folgenden vordefinierten Sicherheitsrollen.

- `eMessage_admin`
- `eMessage_user`

Den Benutzern müssen beide Rollen zugewiesen sein, damit sie auf eMessage-Mailing-Funktionen zugreifen können.

Zugehörige Konzepte:

Kapitel 10, „Verwaltung des Benutzerzugriffs auf Messaging-Funktionen", auf Seite 109

„Rollen- und Richtlinienzuweisung für Mailing-Zugriff" auf Seite 109

Zugehörige Tasks:

„eMessage-Rollen zuweisen" auf Seite 119

eMessage-Rollen zuweisen

Wenn Sie einem Benutzer uneingeschränkten Zugriff auf die Mailing-Funktionen von eMessage erteilen möchten, weisen Sie dem Benutzer die vordefinierten eMessage-Rollen zu.

Vorgehensweise

1. Navigieren Sie in IBM Marketing Platform zu `Settings > User roles & Permissions > eMessage > partition [n] > eMessage_admin` (Einstellungen > Benutzerrollen und Berechtigungen > eMessage > Partition [n] > eMessage_admin).
2. Klicken Sie auf **Assign Users** (Benutzer zuweisen).
3. Wählen Sie den Benutzer in der Liste der verfügbaren Benutzer aus. Klicken Sie auf **Add** (Hinzufügen), um die Rolle dem Benutzer zuzuweisen.
4. Wiederholen Sie die Schritte 1 bis 3 für die Rolle `eMessage_user`.
5. Änderungen speichern.

Zugehörige Konzepte:

„Nachrichtenberechtigungen für eMessage" auf Seite 118

E-Mail-Domänen und Kurzlinkdomänen

Auf Anfrage konfiguriert IBM eine oder mehrere E-Mail-Domänen für Ihr gehostetes E-Mail-Konto. IBM kann auch Domänen zuweisen, mit denen Marketiers in verschiedenen Nachrichtentypen verkürzte Links erstellen. Systemadministratoren mit entsprechenden Berechtigungen verwalten die Nachrichtendomänen, die Marketiers zur Verfügung stehen.

Informationen zu diesem Vorgang

Abhängig von Ihren Geschäftsanforderungen ist es unter Umständen wünschenswert, die Liste der Nachrichtendomänen zu begrenzen, die bestimmten Marketiers zur Verfügung stehen. eMessage-Administratoren schränken die Liste der verfügbaren Domänen mithilfe von Sicherheitsrichtlinien ein, die für Ordner im Document Composer angewendet werden. Ob Marketiers E-Mail-Kommunikationen erstellen und bearbeiten können, hängt von den Sicherheitsrichtlinien ab, die für den Ordner gelten, in dem die Kommunikationen enthalten sind.

eMessage-Administratoren mit den entsprechenden Berechtigungen können die Liste der E-Mail-Domänen steuern, die eMessage-Benutzer als Domäne **Von:** in E-Mail-Kommunikationen verwenden können. Administratoren können auch die Liste der Kurzlinkdomänen steuern, die Marketiers bei der Konfiguration von Kommunikationen angezeigt werden, in denenekürzte Links verwendet werden sollen. So können Sie beispielsweise die Kurzlinkdomänen angeben, die zur Auswahl stehen, wenn Marketer Marketing-Nachrichten einen Link zum Teilen in sozialen Netzen hinzufügen.

eMessage-Administratoren können über die Seite **Richtlinieneinstellungen** Berechtigungen für die Verwendung spezifischer Messaging-Domänen erteilen. Der Zugriff auf die Seite **Richtlinieneinstellungen** wird über die Berechtigungen für die E-Mail-Verwaltung gesteuert, die über die globale Campaign-Richtlinie erteilt werden. Nur Administratoren mit den entsprechenden Berechtigungen können den Zugriff auf E-Mail-Domänen über die Seite **Richtlinieneinstellungen** einschränken.

Vorgehensweise

1. Wählen Sie im Menü **Einstellungen** die eMessage-Einstellungen aus. Wenn Sie über die entsprechenden Administratorberechtigungen verfügen, wird auf der Seite 'eMessage-Einstellungen' der Abschnitt 'Richtlinieneinstellungen' angezeigt.
2. Klicken Sie auf **Liste der Richtlinien und ihrer Einstellungen anzeigen**. Es wird eine Liste der Sicherheitsrichtlinien angezeigt, die für Ihre eMessage-Installation konfiguriert werden.
3. Klicken Sie auf die Sicherheitsrichtlinie, die dem Systembenutzer zugeordnet ist, für den der Zugriff auf die Messaging-Domäne gesteuert werden soll.

   Im Abschnitt 'Domänen' werden die E-Mail-Domänen angezeigt, die für Ihr gehostetes Messaging-Konto konfiguriert sind.

   Im Abschnitt 'Kurzlinkdomänen' werden die Kurzlinkdomänen angezeigt, die für Ihr gehostetes Messaging-Konto konfiguriert sind.

   - Klicken Sie in einem dieser Abschnitte auf **Alle Domänen verwenden**, damit Benutzer, die dieser Richtlinie zugeordnet sind, alle E-Mail-Domänen verwenden können, die IBM für Ihr gehostetes E-Mail-Konto konfiguriert hat.

     Diese Option ist die Standardeinstellung.
   - Klicken Sie auf **Bestimmte Domänen verwenden**, um bestimmte Domänen auszuwählen.

     Anmerkung: Bei Auswahl von **Bestimmte Domänen verwenden** müssen Sie die Domänenberechtigungen aktualisieren, wenn Sie eine neue E-Mail- oder Kurzlinkdomäne für Ihr gehostetes Messaging-Konto registrieren. Der neuen Domäne werden Berechtigungen nicht automatisch vom System zugewiesen.

Ergebnisse

Für Benutzer, die der Sicherheitsrichtlinie zugeordnet sind, stehen als **Von:**-Adresse in E-Mail-Kommunikationen nur die ausgewählten E-Mail-Domänen zur Auswahl. Für Kommunikationen, für die gekürzte Links erforderlich sind, können Marketiers nur unter den von Ihnen ausgewählten Kurzlinkdomänen wählen.

Nachdem Sie die neuen Einstellungen gespeichert haben, werden die für Marketiers verfügbaren Domänenoptionen vom Document Composer aktualisiert.

Weitere Informationen dazu, wie eMessage-Marketiers Kommunikationen erstellen und verwalten, finden Sie im *IBM eMessage-Benutzerhandbuch*.

Wartung von gehosteten E-Mail-Domänen

Um E-Mail-Nachrichten senden zu können, müssen Sie mindestens eine E-Mail bei IBM registrieren. Um die Zustellbarkeit von Nachrichten zu verbessern, hilft IBM Ihnen dabei, die E-Mail-Reputation der Domäne bei führenden Internet-Service-Providern (ISPs) auf der ganzen Welt aufzubauen und aufrechtzuerhalten. Sie können mehrere E-Mail-Domänen bei IBM einrichten.

Wenn Sie die Kopfzeile in einer E-Mail-Kommunikation konfigurieren, füllt das System die Absenderadresse mit der E-Mail-Domäne, die Sie bei IBM registriert haben. Wenn Sie mehrere E-Mail-Domänen bei IBM einrichten, werden die verfügbaren Domänen in einer Dropdown-Liste angezeigt. Systemadministratoren können steuern, welche E-Mail-Domänen E-Mail-Marketer auswählen oder ändern können.

Sie können IBM bitten, E-Mail-Domänen für Ihr gehostetes Messaging-Konto hinzuzufügen bzw. E-Mail-Domänen zu löschen, die für Ihr gehostetes Messaging-Konto eingerichtet wurden. Nachdem IBM die angeforderten Änderungen vorgenommen hat, wird die Liste der verfügbaren E-Mail-Domänen vom System aktualisiert. Die Änderung ist in der Liste mit verfügbaren E-Mail-Domänen sichtbar, wenn Sie das nächste Mal eine E-Mail-Kommunikation erstellen oder bearbeiten.

Anmerkung: Bei Änderungen der E-Mail-Domänen für Ihr Konto werden E-Mail-Kommunikationen, die Sie vor der Änderungsanforderung erstellt haben, nicht aktualisiert. Um die E-Mail-Domäne einer früher erstellen Kommunikation zu ändern, müssen Sie die E-Mail-Kommunikation erneut öffnen und die Auswahl der E-Mail-Domäne aktualisieren.

Weitere Informationen zur Registrierung einer E-Mail-Domäne bei IBM finden Sie unter *IBM Enterprise Marketing Management (EMM) Domain Name Options for Email*

Wenn Sie Änderungen bezüglich Ihrer E-Mail-Domänen anfordern möchten, wenden Sie sich an das Email Account Services-Team unter `eacctsvc@us.ibm.com`.

Standardabsenderadresse und Anzeigenamen konfigurieren

Sie können für jede E-Mail-Domäne, die Sie bei IBM registriert haben, eine Standard-E-Mail-Adresse und einen Standardanzeigenamen definieren. Die Kombination aus E-Mail-Adresse bzw. Anzeigename und E-Mail-Domäne wird als Absenderadresse (Von:) für die E-Mail-Nachrichten angezeigt, die Sie senden.

Informationen zu diesem Vorgang

Administratoren können die Standardabsender- und Anzeigenamen auf der Seite für Domäneneinstellungen konfigurieren. Die Domäneneinstellungen sind Teil der eMessage-Schnittstelle für Einstellungen. Der Zugriff auf die Seite 'Domäneneinstellungen' wird über die Berechtigungen für die E-Mail-Verwaltung gesteuert, die über die globale Campaign-Richtlinie erteilt werden. Nur Administratoren mit den entsprechenden Berechtigungen können den Zugriff auf E-Mail-Domänen über die Seite 'Richtlinieneinstellungen' einschränken.

Vorgehensweise

1. Rufen Sie **Einstellungen** > **eMessage-Einstellungen** auf. Klicken Sie im Abschnitt für Domäneneinstellungen auf **Anzeige**, um die Liste mit Domäneneinstellungen anzuzeigen.

   Auf der Seite für Domäneneinstellungen werden die Standardanzeigenamen und Standard-E-Mail-Adressen aufgelistet, die den E-Mail-Domänen zugeordnet sind, die für Ihr gehostetes E-Mail-Konto registriert sind. Die Liste enthält nur die Domänen, die Sie aufgrund Ihrer Benutzerberechtigungen ändern können.

   Die Spalte 'Standard' enthält die Kombination aus Anzeigename, Adresse und Domäne, die als Standardabsenderadresse für neue E-Mail-Kommunikationen angezeigt wird.

2. Klicken Sie auf **Bearbeiten** . Das Fenster zur Bearbeitung der Domäneneinstellungen wird geöffnet.

   In der Spalte mit den Domänennamen werden die verfügbaren E-Mail-Domänen aufgelistet. Sie können für jede der Domänen folgende Aktionen ausführen:

- Geben Sie in der Spalte 'Absenderanzeigename' einen Anzeigenamen ein, der als Standardwert für eine E-Mail-Domäne in der Liste aufgeführt werden soll.
- Geben Sie in der Spalte 'Absenderadresse' den lokalen Teil der E-Mail-Adresse ein, der als Standardwert für eine E-Mail-Domäne in der Liste aufgeführt werden soll.

3. Wählen Sie optional in der Spalte 'Standard' eine Kombination aus Anzeigename, Adresse und Domäne aus, die als Standardabsenderadresse für neue E-Mail-Kommunikationen angezeigt werden soll.

   Wenn Sie keinen Standardwert auswählen, verwendet das System die erste Domäne in der Liste, um die Standardabsenderadresse für neue E-Mail-Kommunikationen zu erstellen.
4. Speichern Sie die Änderungen.

Ergebnisse

Die neuen Adresseinstellungen gelten für alle neuen E-Mail-Kommunikationen, die Sie erstellen. Adressinformationen für E-Mail-Kommunikationen, die Sie bereits erstellt haben, werden durch die Einstellungen nicht geändert. Um ältere E-Mail-Kommunikationen zu aktualisieren, müssen Sie jede Kommunikation erneut öffnen und ändern.

Steuerung des Zugriffs auf die Liste gesendeter Nachrichten

eMessage stellt eine Liste der Nachrichten zur Verfügung, die von Ihrer eMessage-Umgebung gesendet wurden. Da die Liste auch Links zu Messaging-Konfigurationen enthält, müssen Sie den Zugriff auf die Liste abhängig von Ihren Sicherheitsplänen möglicherweise einschränken.

Informationen zu diesem Vorgang

Die Liste der Nachrichten wird auf der Seite **eMessage-Mailings** angezeigt. Standardmäßig können alle Benutzer in Ihrer Campaign- und eMessage-Umgebung die Liste der gesendeten Nachrichten sehen. Wenn Sie jedoch die Zugriffsbeschränkung aktivieren, können Sie verhindern, dass bestimmte Benutzer die Menüoption für das Öffnen der Seite, die die Liste enthält, sehen.

Die Einschränkung des Zugriffs auf die Liste der gesendeten Nachrichten wirkt sich auf alle Partitionen in Ihrer Campaign-Installation aus. Wenn Ihre Campaign-Installation mehrere Partitionen enthält, müssen Sie die Benutzerberechtigungen in jeder Partition separat aktualisieren, um die Zugriffsberechtigung für die Liste explizit zu erteilen oder zu verweigern.

Zur Steuerung des Zugriffs auf die Liste der gesendeten Nachrichten müssen mehrere Aufgaben ausgeführt werden, mit denen die Benutzerberechtigungen und die Systemkonfiguration geändert werden.

Aufgabe	Weitere Informationen
Identifizieren Sie Benutzer, die auf die Liste der Nachrichten zugreifen können. Zu Beginn können alle Benutzer darauf zugreifen.	„Zugriff auf die Liste gesendeter Nachrichten erteilen" auf Seite 123
Identifizieren Sie Benutzer, die nicht auf die Liste der Nachrichten zugreifen dürfen.	„Zugriff auf die Liste gesendeter Nachrichten verweigern" auf Seite 124

Aufgabe	Weitere Informationen
Aktivieren Sie die Zugriffsbeschränkung.	„Einschränkung für die Liste gesendeter Nachrichten aktivieren" auf Seite 125

Ergebnisse

Wenn Sie diese Tasks vollständig ausgeführt haben, ist die Option **eMessage-Mailings** im Menü **Kampagne** nur für Benutzer sichtbar, deren Rollen ihnen den Zugriff auf die Mailing-Liste explizit erlauben.

Zugriff auf die Liste gesendeter Nachrichten erteilen

Wenn Sie den Zugriff auf die Liste der gesendeten Nachrichten einschränken, müssen Sie Benutzern, die Zugriff auf die Liste erhalten sollen, den Zugriff explizit erteilen.

Informationen zu diesem Vorgang

Benutzer können über den Link **eMessage-Mailings** im Menü **Kampagne** auf die Liste gesendeter Nachrichten zugreifen. Sie können einem Benutzer Zugriff auf die Liste mit allen gesendeten Nachrichten erteilen, indem Sie dem Benutzer eine Verwaltungsrolle auf höchster Ebene zuweisen, der explizit die Berechtigung zur Anzeige des Links **eMessage-Mailings** erteilt ist.

Zu den Standardrollen der höchsten Ebene zählen **Verwalten**, **Ausführen**, **Design** und **Überprüfen**. Die Berechtigungen, die Sie über die Rollen der höchsten Ebene erteilen, gelten für alle Objekte in der Partition.

Vorgehensweise

1. Rufen Sie `Settings > User Roles and Permissions > Campaign > partition (n)` (Einstellungen > Benutzerrollen und Berechtigungen > Campaign (Partition (n)) auf.
2. Klicken Sie auf **Save and Edit Permissions** (Berechtigungen speichern und bearbeiten). Es wird eine Liste mit den Berechtigungen für die Partition geöffnet. Die verfügbaren Rollen der höchsten Ebene werden oben auf der Seite aufgelistet.
3. Erteilen Sie jeder Rolle im Abschnitt **Verwaltung** explizit die Berechtigung **Seite mit Mailing-Liste anzeigen**.

Ergebnisse

Wenn Sie Zugriffsbeschränkungen für die Liste gesendeter Nachrichten aktivieren, können Benutzer mit Rollen, denen explizit die Berechtigung **Seite mit Mailing-Liste anzeigen** erteilt wurde, den Link **eMessage-Mailings** im Menü **Kampagne** sehen.

Nächste Schritte

Erstellen Sie eine Rolle, um den Zugriff auf die Liste der gesendeten Mailings zu verweigern.

Zugehörige Tasks:

„Zugriff auf die Liste gesendeter Nachrichten verweigern" auf Seite 124

„Einschränkung für die Liste gesendeter Nachrichten aktivieren" auf Seite 125

Zugriff auf die Liste gesendeter Nachrichten verweigern

Wenn Sie den Zugriff auf die Liste der gesendeten Nachrichten einschränken, müssen Sie Benutzern, die keinen Zugriff auf die Liste erhalten sollen, den Zugriff explizit verweigern.

Informationen zu diesem Vorgang

Benutzer können über den Link **eMessage-Mailings** im Menü **Kampagne** auf die Liste gesendeter Nachrichten zugreifen. Sie können einem Benutzer den Zugriff auf die Liste mit allen gesendeten Nachrichten verweigern, indem Sie dem Benutzer eine Verwaltungsrolle auf höchster Ebene zuweisen, der explizit die Berechtigung zur Anzeige des Links **eMessage-Mailings** verweigert ist.

Zu den Standardrollen der höchsten Ebene zählen **Verwalten**, **Ausführen**, **Design** und **Überprüfen**. Die Berechtigungen, die Sie über die Rollen der höchsten Ebene erteilen, gelten für alle Objekte in der Partition. Sie können neue Rollen der höchsten Ebene erstellen, um die Standardrollen der höchsten Ebene zu ergänzen. Die neuen Rollen können bestimmte Berechtigungen erteilen oder verweigern.

Vorgehensweise

1. Rufen Sie **Settings** > **User Roles and Permissions** > **Campaign** > **partition (n)** (Einstellungen > Benutzerrollen und Berechtigungen > Campaign > Partition (n)) auf. Daraufhin wird die Seite **partition <n>** geöffnet.
2. Klicken Sie auf **Add Role** (Rolle hinzufügen). Weisen Sie der Rolle einen Namen zu und geben Sie eine Kurzbeschreibung ein. Speichern Sie die Änderungen und kehren Sie zur Seite **partition <n>** zurück.
3. Konfigurieren Sie die neue Rolle, um den Zugriff auf die Liste der gesendeten Mailings zu verweigern.
   a. Klicken Sie auf **Add Roles and Assign Permissions** (Rollen hinzufügen und Berechtigungen zuweisen). Daraufhin wird die Seite **Properties for Administrative Roles** (Eigenschaften für Verwaltungsrollen) geöffnet. Die neue Rolle wird in der Liste der Rollen angezeigt.
   b. Klicken Sie auf **Save and Edit Permissions** (Berechtigungen speichern und bearbeiten). Eine Liste der Berechtigungen für die Partition wird als Matrix mit Auswahlsymbolen angezeigt, die den Status der einzelnen Berechtigungen für jede Rolle anzeigen. Die neue Rolle wird oben in der Matrix neben den anderen Rollen der höchsten Ebene angezeigt.
   c. Verweigern Sie der neuen Rolle im Abschnitt **Verwaltung** explizit die Berechtigung **Seite mit Mailing-Liste anzeigen**. Speichern Sie die Änderungen.
4. Weisen Sie die neue Rolle den Benutzern zu, die keinen Zugriff auf die Mailing-Listenseite erhalten sollen.
   a. Rufen Sie **Settings** > **Users** (Einstellungen > Benutzer) auf. Wählen Sie den Benutzer aus, bei dem Sie den Zugriff auf die Liste der gesendeten Nachrichten verhindern möchten.
   b. Klicken Sie auf **Edit Roles** (Rollen bearbeiten). Die neue Rolle, die Sie im vorherigen Schritt erstellt haben (eine Rolle, für die eine Zugriffsverweigerung konfiguriert wurde), wird in der Liste **Available Roles** (Verfügbare Rollen) angezeigt.
   c. Verschieben Sie die neue Rolle aus **Available Roles** (Verfügbare Rollen) in **Roles** (Rollen). Änderungen speichern.

Ergebnisse

Wenn Sie die Zugriffsbeschränkungen für die Liste gesendeter Nachrichten aktivieren, kann ein Benutzer, dem die neue Rolle zugewiesen wurde, den Link **eMessage-Mailings** nicht sehen.

Nächste Schritte

Aktualisieren Sie die Konfiguration, um die Zugriffsbeschränkungen für die Liste der gesendeten Nachrichten zu aktivieren.

Zugehörige Tasks:

„Zugriff auf die Liste gesendeter Nachrichten erteilen" auf Seite 123

„Einschränkung für die Liste gesendeter Nachrichten aktivieren"

Einschränkung für die Liste gesendeter Nachrichten aktivieren

Benutzer können über die Option **eMessage-Mailings** im Menü **Kampagne** auf die Liste gesendeter Nachrichten zugreifen. Wenn Sie den Zugriff auf die Liste der gesendeten Nachrichten einschränken, steuert die Eigenschaft `Security Function ID` (Sicherheitsfunktions-ID) die Anzeige dieser Menüoption und damit auch den Zugriff auf die Liste der gesendeten Nachrichten.

Informationen zu diesem Vorgang

Wenn Sie den Zugriff auf die Liste der gesendeten Nachrichten einschränken, müssen Sie die Eigenschaft `Security Function ID` (Sicherheitsfunktions-ID) in der Marketing Platform-Konfiguration aktualisieren. Diese Eigenschaft gilt für alle Partitionen in Ihrer Installation von Campaign.

Wenn Sie die Sicherheitsfunktions-ID mit dem richtigen Wert belegen, ist die Option **eMessage-Mailings** nur für Benutzer mit einer Rolle verfügbar, die ihnen explizit die Berechtigung zur Anzeige der Mailing-Listenseite erteilt. Benutzer mit Rollen, bei denen die Berechtigung zur Anzeige der Mailing-Listenseite entweder verweigert oder nicht erteilt wurde, können die Option **eMessage-Mailings** nicht sehen.

Vorgehensweise

1. Rufen Sie **Settings** > **Configuration** > **Platform** > **Platform-wide navigation** > **Main navigation menu** > **Campaign** > **eMessage Mailings** (Einstellungen > Konfiguration > Plattform > Plattformweite Konfiguration > Hauptnavigationsmenü > Campaign > eMessage-Mailings) auf. Klicken Sie auf **eMessage-Mailings**, um die Konfigurationseinstellungen anzuzeigen.
2. Klicken Sie auf **Edit Settings** (Einstellungen bearbeiten).
3. Geben Sie im Feld **Security Function ID** (Sicherheitsfunktions-ID) den Wert `7000` ein. Änderungen speichern.

   Um die Ergebnisse der Konfigurationsänderung sehen zu können, müssen Sie sich vom System abmelden und erneut anmelden.

Ergebnisse

Nur Benutzer mit Rollen, die explizit die Berechtigung für die Anzeige der Mailing-Listenseite erteilen, können den Link **eMessage-Mailings** sehen, über den ein Zugriff auf die Liste gesendeter Nachrichten möglich ist.

Zugehörige Tasks:

„Zugriff auf die Liste gesendeter Nachrichten erteilen" auf Seite 123

„Zugriff auf die Liste gesendeter Nachrichten verweigern" auf Seite 124

Berechtigungen für eMessage-Berichte

Über Ihre Benutzerberechtigungen wird festgelegt, ob Sie eMessage-Berichte anzeigen können.

Informationen zum Festlegen von Berechtigungen für den Zugriff auf eMessage-Standardberichte finden Sie im Abschnitt zur Berichterstellung und Sicherheit im *IBM EMM Reports Installations- und Konfigurationshandbuch*.

Bevor Sie sich an den IBM Technical Support wenden

Wenn ein Problem auftritt, das Sie mithilfe der Dokumentation nicht lösen können, kann die für den Support zuständige Kontaktperson Ihres Unternehmens ein Gespräch mit dem IBM Technical Support protokollieren. Gehen Sie entsprechend diesen Leitlinien vor, um sicherzustellen, dass Ihr Problem effizient und erfolgreich gelöst wird.

Wenn in Ihrem Unternehmen keine für den Support zuständige Kontaktperson ist, wenden Sie sich für Informationen an Ihren IBM Administrator.

Anmerkung: Der Technical Support schreibt oder erstellt keine API-Scripts. Um Unterstützung bei der Implementierung unserer API-Angebote zu erhalten, wenden Sie sich an IBM Professional Services.

Erforderliche Informationen

Bevor Sie sich an den IBM Technical Support wenden, halten Sie folgende Informationen bereit:

- Eine kurze Beschreibung der Art Ihres Problems.
- Ausführliche Fehlernachrichten, die beim Auftreten des Problems angezeigt werden.
- Ausführliche Schritte, um das Problem zu reproduzieren.
- Zugehörige Protokolldateien, Sitzungsdateien, Konfigurationsdateien und Datendateien.
- Informationen zu Ihrem -Produkt und Ihrer Systemumgebung. Sie finden diese entsprechend der Beschreibung unter "Systeminformationen".

Systeminformationen

Wenn Sie IBM Technical Support anrufen, werden Sie unter Umständen gebeten, Informationen zu Ihrer Umgebung bereitzustellen.

Wenn Sie sich trotz des Problems anmelden können, sind viele dieser Informationen auf der Seite **About** (Produktinformation) verfügbar, die Informationen zu Ihren installierten IBM Anwendungen enthält.

Sie können auf die Seite **About** (Produktinformation) zugreifen, indem Sie **Help > About** (Hilfe > Produktinformation) auswählen. Ist kein Zugriff auf die Seite **About** (Produktinformation) möglich, suchen Sie nach der Datei `version.txt`, die sich im Installationsverzeichnis Ihrer Anwendung befindet.

Kontaktinformationen für IBM Technical Support

Kontaktmöglichkeiten zu IBM Technical Support finden Sie auf derIBM Product Technical Support-Website: (http://www.ibm.com/support/entry/portal/open_service_request).

Anmerkung: Um eine Supportanfrage einzugeben, müssen Sie sich mit einem IBM Konto anmelden. Dieses Konto muss mit Ihrer IBM Kundennummer verknüpft sein. Weitere Informationen zur Zuordnung Ihres Kontos zu Ihrer IBM Kunden-

© Copyright IBM Corp. 1999, 2015

nummer finden Sie unter **Support Resources > Entitled Software Support** (Support-Ressourcen > Berechtigter IBM Software Support) im Support-Portal.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
B1WA LKG1

© Copyright IBM Corp. 1999, 2015

550 King Street
Littleton, MA 01460-1250
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können unter Umständen von den hier genannten Preisen abweichen.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellensprache geschrieben sind und Programmiertechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten. Die Beispielprogramme werden ohne Wartung (auf "as-is"-Basis)

und ohne jegliche Gewährleistung zur Verfügung gestellt. IBM übernimmt keine Haftung für Schäden, die durch die Verwendung der Beispielprogramme entstehen.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM Corp in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Hinweise zu Datenschutzrichtlinien und Nutzungsbedingungen

IBM Softwareprodukte, einschließlich Software as a Service-Lösungen ("Softwareangebote"), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. Ein Cookie ist ein Datenelement, das von einer Website an Ihren Browser gesendet wird und dann als Tag auf Ihrem Computer gespeichert werden kann, mit dem Ihr Computer identifiziert wird. In vielen Fällen werden von diesen Cookies keine personenbezogenen Daten erfasst. Wenn ein Softwareangebot, das von Ihnen verwendet wird, die Erfassung personenbezogener Daten anhand von Cookies und ähnlichen Technologien ermöglicht, werden Sie im Folgenden über die hierbei geltenden Besonderheiten informiert.

Abhängig von den bereitgestellten Konfigurationen kann dieses Softwareangebot Sitzungscookies und permanente Cookies verwenden, mit denen der Benutzername des Benutzers und andere personenbezogene Daten zum Zwecke des Sitzungsmanagements, zur Verbesserung der Benutzerfreundlichkeit und zu anderen funktionsbezogenen Zwecken sowie zur Nutzungsüberwachung erfasst werden. Diese Cookies können deaktiviert werden. Durch die Deaktivierung kann jedoch auch die von ihnen bereitgestellte Funktionalität nicht mehr genutzt werden.

Die Erfassung personenbezogener Daten mithilfe von Cookies und ähnlichen Technologien wird durch verschiedene rechtliche Bestimmungen geregelt. Wenn die für dieses Softwareangebot implementierten Konfigurationen Ihnen als Kunde die Möglichkeit bieten, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, dann sollten Sie ggf. juristische Beratung zu den geltenden Gesetzen für eine solche Datenerfassung in Anspruch nehmen. Dies gilt auch in Bezug auf die Anforderungen, die vom Gesetzgeber in Bezug auf Hinweise und die Einholung von Einwilligungen vorgeschrieben werden.

IBM setzt voraus, dass Kunden (1) einen deutlich sichtbaren Link zu ihren Nutzungsbedingungen auf ihrer Website (z. B. Datenschutzrichtlinie) bereitstellen, die wiederum einen Link zur Praxis der Datenerfassung und -verwendung bei IBM und beim Kunden beinhaltet, (2) darauf hinweisen, dass IBM für den Kunden Cookies und Clear GIFs/Web-Beacons auf dem Computer des Kunden platziert, und (3), soweit dies gesetzlich vorgeschrieben ist, vor der Platzierung von Cookies und Clear GIFs/Web-Beacons auf den Geräten von Website-Besuchern durch den Kunden selbst oder für den Kunden durch IBM die Einwilligung des jeweiligen Website-Besuchers einholen.

Weitere Informationen zur Verwendung verschiedener Technologien einschließlich der Verwendung von Cookies zu diesen Zwecken finden Sie im IBM Online Privacy Statement unter der Webadresse http://www.ibm.com/privacy/details/us/en

im Abschnitt mit dem Titel "Cookies, Web Beacons and Other Technologies".